



DIGICAB



AI & PRIVACY

Eduardo López-Román

Digital Lawyer & DPO (AI specialist)

(SPAIN - Barcelona)

Twitter: @edulawyer

E-mail: eduardlr@icab.cat



1.- Artificial Intelligence

(“Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE – APRIL 2021 - **ARTIFICIAL INTELLIGENCE ACT**”)

Privacy

(“GENERAL DATA PROTECTION REGULATION - **GDPR**”)



2.- Artificial intelligence depends on (personal) data processing.

DATA, THE RAW MATERIAL OF ARTIFICIAL INTELLIGENCE.



3.- The AI Act follows a risk-based approach, differentiating between uses of AI that create:

- (i) an unacceptable risk,***
- (ii) a high risk, and***
- (iii) low or minimal risk.***



4.- The proposal also contains specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons.



5.- *There is identified two main categories of high-risk AI systems:*

- *AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment;*
- *other stand-alone AI systems with mainly fundamental rights implications that will be explicitly listed in the future Regulation.*



6.- AI RISK ASSESSMENT METHODOLOGY AND DATA PROTECTION IMPACT ASSESSMENT.

To ensure that the regulation can be adjusted to emerging uses and applications of AI, the Commission could expand the list of high-risk AI systems used within certain pre-defined areas, by applying a set of criteria and risk assessment methodology.



7.- TRANSPARENCY:

Prop. AI Act: *“Transparency obligations should be applied for systems that (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content (‘deep fakes’).”*

GDPR: Principles relating to processing of personal data. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**).



8.- “Privacy by Design”:

Article 25 GDPR

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying **likelihood and severity for rights and freedoms of natural persons posed by the processing**, 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, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.



9.- GDPR Compliance: the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.



DIGICAB



THANK YOU

Eduardo López-Román

Twitter: @edulawyer

E-mail: eduardlr@icab.cat