Artificial “Intelligence”

Data Privacy Day University of Luxembourg:
29 January 2024

Raoul Winkens, Data Protection Officer Maastricht University & Sandrine Munoz Data Protection Officer University Luxembourg

Maastricht University

Introduction

Who: Raoul Winkens

- Data Protection Officer @ Maastricht University since 2018
- Lawyer interested in technology, education and research with a focus on data protection

What:

- How should academia tackle technological advancement with a focus on AI?

Connect:

- LinkedIn
- raoul.winkens@maastrichtuniversity.nl

Introduction

- How does AI and upcoming legislation interact with GDPR and the academic sector?
- Tasks of the DPO: “to monitor compliance with this Regulation, with other Union or Member State data protection provisions(…)”
- GDPR mentions the word ‘risk’ more than 70 times and the word ‘privacy’ 0 times (once in a footnote).
- AI and the AI-act is all about risk and risk assessment.

EU: fit for the digital age / data strategy / Digital Decade: https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

Table 1: Overview of EU Legislation in the Digital Sector

Applicable law	Published in the Official Journal of the European Union
In negotation	Proposal by the European Commission entered the legislative process.
Planed initiative	Mentioned by the European Commission as potential legislative initiative

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	General Data Protection Regulation (GDPR), (EU) 2016/679	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	Technology Transfer Block Exemption, (EC) 2014/316	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Information Society Directive, (EC) 2001/29	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation on the free flow of non-personal data, (EU) 2018/1807	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1172	Open Internet Access Regulation, (EU) 2015/2120	Open Data Directive (PSI), (EU) 2019/1024	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Portability Regulation, (EU) 2017/1128	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Cybersecurity Regulation, 2022/0085(COD)	E-evidence Regulation, 2018/0108(COD)	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	Satellite and Cable II Directive, (EU) 2019/789	Digital euro, 2023/0212 (COD)
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Design Directive, 2022/0392(COD)	Cyber Resilience Act, 2022/0272(COD)	Digitalization of travel documents	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), 2022/0032(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)	Compulsory licensing of patents, 2023/0129(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)		Machinery Regulation, (EU) 2023/1230	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	.eu top-level domain Regulation, (EU) 2019/517	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2022/1066, (EU) 2023/1067		Revision of the late payments Directive
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	New radio spectrum policy programme (RSPP 2.0)	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
		Telecoms Act / Fair Share initiative	Harmonization of GDPR enforcement 2023/0202(COD)				AI Liability Directive, 2022/0303(COD)	Right to repair Directive, 2023/0083(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		
			Interoperable Europe Act, 2022/0379(COD)					Political Advertising Regulation, 2021/0381(COD)			
			Access to vehicle data, functions and resources					Multimodal digital mobility services (MDMS)			
			GreenData4all					Consumer protection: strengthened enforcement cooperation			
								Consumer rights: adapting ADR to digital markets			

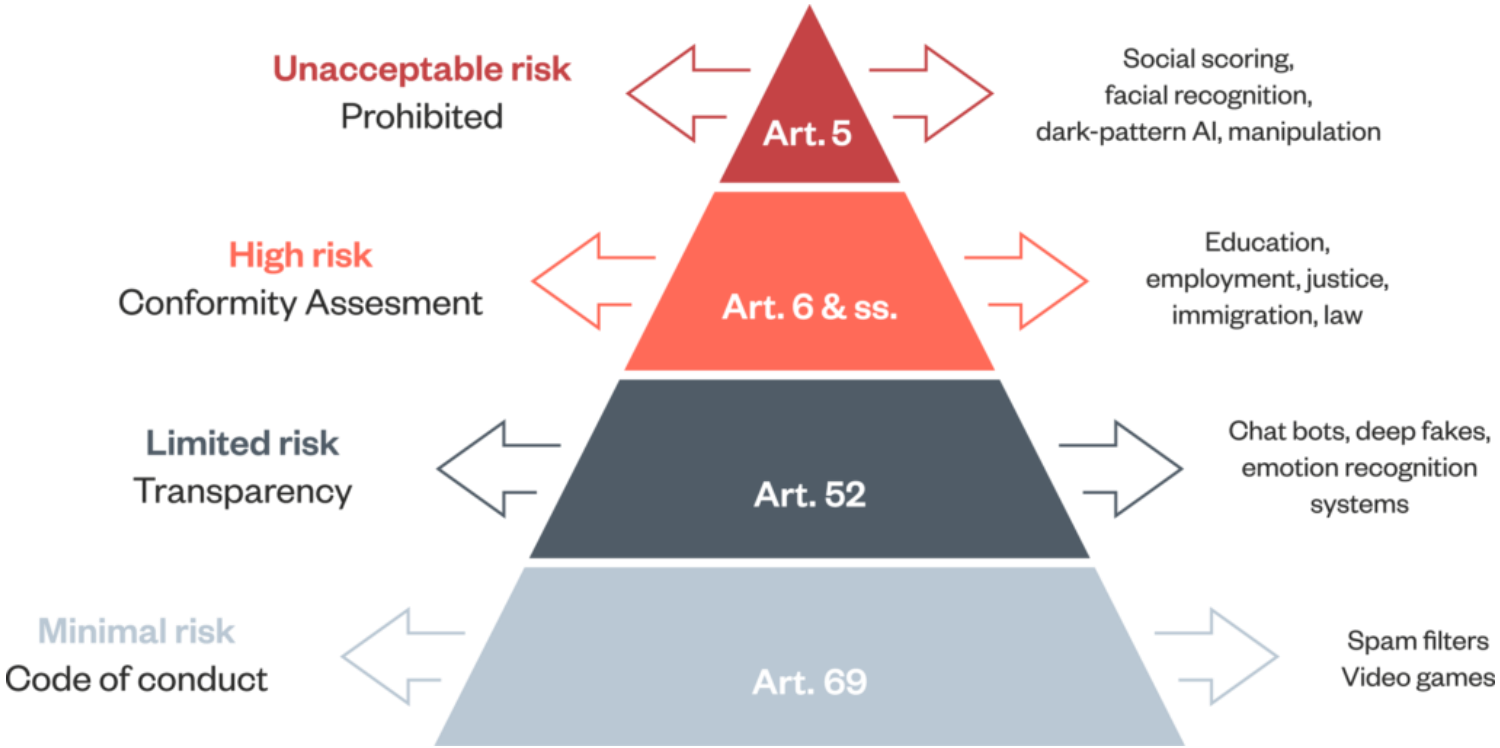
kaizenner.eu

bruegel

AI-Act (definition European Parliament)

EP: “[An] ‘artificial intelligence system’ (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.”

AI-Act (proposal)



Source: https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/

AI-Act (proposal)

Source: https://futurium.ec.europa.eu/hr/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act?language=hr

And what does that mean for me?

- Can I use AI (tooling, systems) in my research?
- How can I identify risks?
- What level of detail is needed?

Answers?

Does any (popular) AI application in use now comply with the AI act proposal?

Data protection authorities are also becoming responsible for AI/algorithm oversight

GDPR is technology neutral and will remain relevant (still fit for purpose?)

'I was shocked it was so easy': meet the professor who says facial recognition can tell if you're gay

Michal Kosinski: 'I don't believe in free will.' Photograph: Jason Henry/The Guardian

Psychologist Michal Kosinski says artificial intelligence can detect your sexuality and politics just by looking at your face. What if he's right?

Vladimir Putin was not in attendance, but his loyal lieutenants were. On 14 July last year, the Russian prime minister, Dmitry Medvedev, and several members of his cabinet convened in an office building on the outskirts of Moscow. On to the stage stepped a boyish-looking psychologist, Michal Kosinski, who had been

Why AI is concerned by data protection?

- AI generally works and trains with data
  - Composing texts and modules e.g. emails
  - Collecting and evaluating data e.g. applicants CVs, participants data within research projects
  - Training of systems (machine learning)

- AI technologies like machine learning process personal during 2 phases
  - Learning phase
  - Operational phase

Why AI is concerned by data protection?

- When using AI **compliance with data protection laws** is **crucial**
  - As soon as AI process personal data the relevant data protection regulations must be observed
  - **EU Commission 2019**: High-level Expert Group about AI issued ethics guidelines:
    - One of the pilar is lawfulness

https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Why AI is concerned by data protection?

Accountability

If your institution will process personal data with AI techniques the compliance is mandatory and must be documented

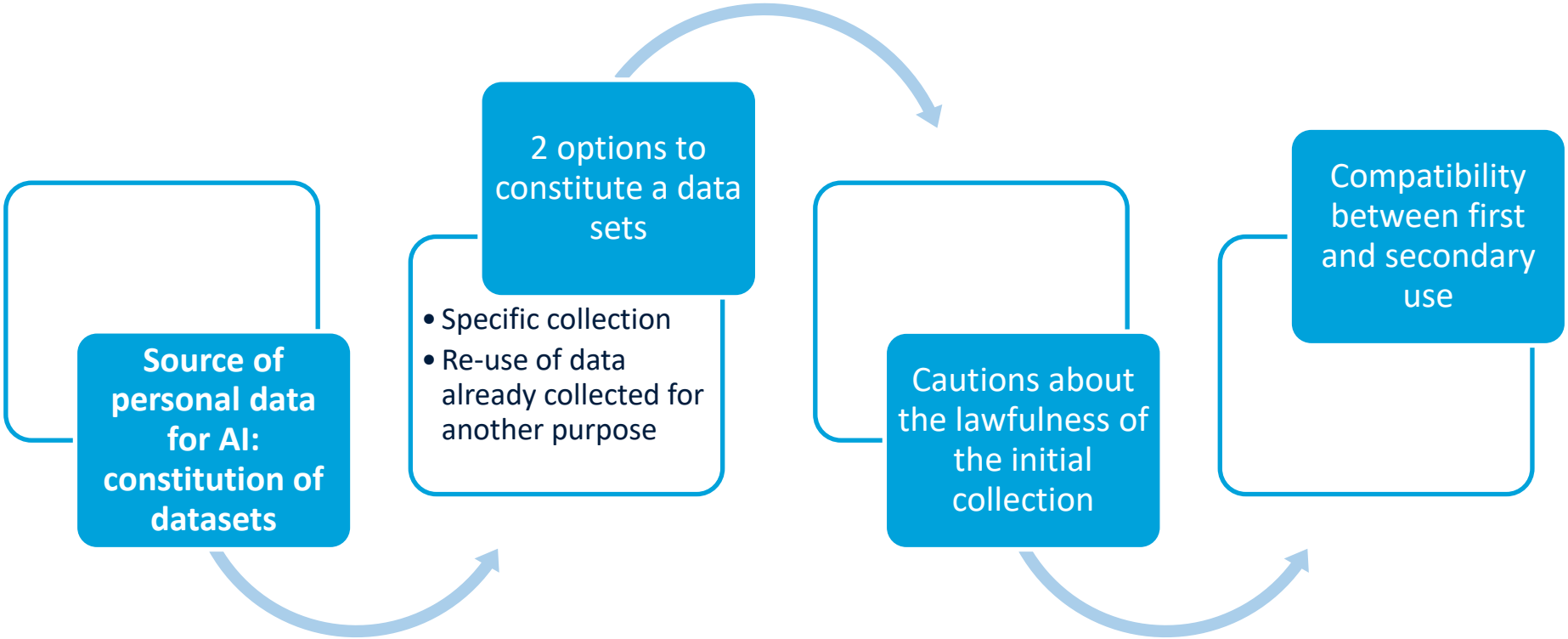
At a glance, which data protection requirements?

- Define a purpose
- Determine a legal basis
- Respect the minimisation principle
- Define a retention period
- Ensure security
- Provide information to data subjects
- Implement the exercise of rights
- Assessing the system
- Avoiding algorithm discrimination

Which data protection requirements?

Processing of personal data must always serve a specific and legitimate purpose	AI system based on the use of personal data must always be developed, trained and deployed with a clear-defined purpose which means clear objective(s)	
	Only relevant data is used	
	At the stage of project design	
Determination a legal basis	The objective of 'scientific research' cannot itself constitute a legal basis	
	6 legal basis within the GDPR (art.6)	
	Opinion of CNIL (French supervisory authority) regarding creation of health data warehouses	As part of public interest missions and for subsequent research

Which data protection requirements?



Which data protection requirements?

Respect data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

AI needs large amount of data

Data minimisation is not itself an obstacle

Which data protection requirements?

Concretely

- If feasible, use **fictitious data** (same structure as real data but not linked to an individual)
- Involve IT staff
- **Understand** and **map** out all the Machine learning processes in which personal data might be used

One example

- Clinical research assessed by the French Data Supervisory authority:
  - ➢ Purposes: identifying explanatory variables for prostate cancer (pharmaceutical lab)
  - ➢ Processing of the entire patient population from the medical records of various centres is disproportionate, no respect of data minimisation principle

Which data protection requirements?

Define a retention period

Personal data **cannot** be stored for **indefinite period**

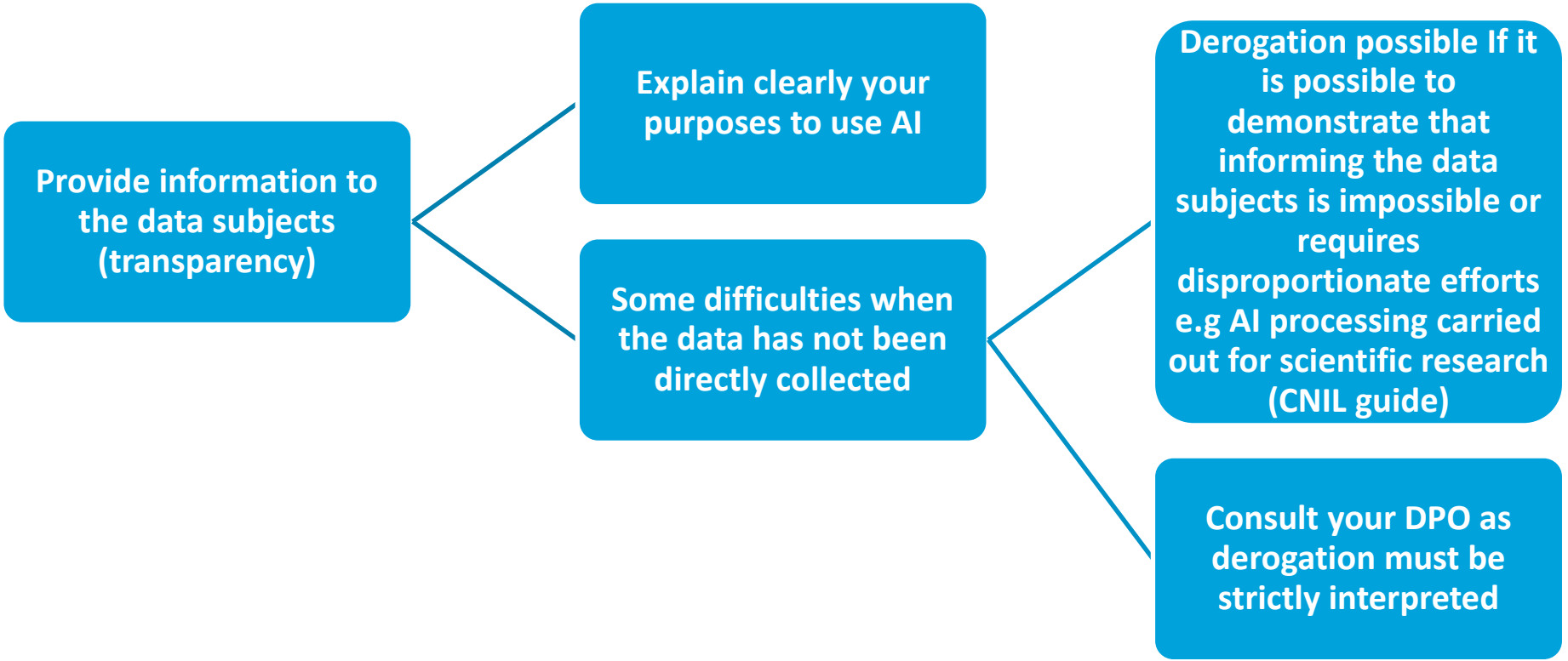
AI requires **longer period of time** than other processings operations e.g. training and developing new systems

Clearly schedule the period for performance measurement

Longer period for example to allow reproducibility in research

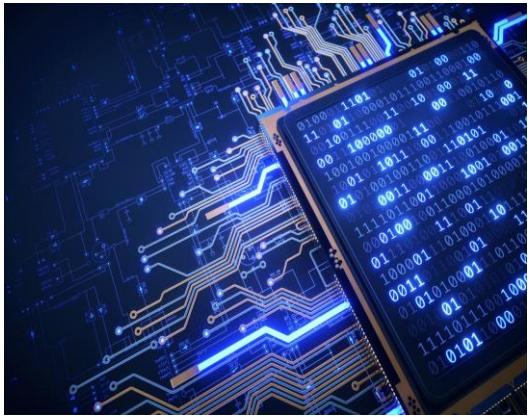
Organisational and technical measures to ensure rights and freedoms of data subjects (participants to research projects)

Which data protection requirements?



Which data protection requirements?

- Most of the AI based processing will **require a risk analysis (DPIA)** to be performed



- Potential Criteria
  - Evaluation and scoring
  - Automated decision making legal or similar effects
  - Sensitive data
  - Data processed at a large scale e.g. machine learning
  - Matching & combining datasets
  - Innovative use or applying new technological solutions

Conclusion?

Legislation will always be behind technological development

Legislation will always be lacking in certain areas

GDPR needs to be taken into account in combination with other legislation

When using AI-technology in combination with personal data take caution and consult your DPO

Thank you!