Digdir

digdir.no

EU-regelverk om deling av data og KI

Fagforum
30.09.2022

Heather Broomfield og Maren Stefansen
Nasjonalt ressurssenter for deling og bruk av data
Digitaliseringsdirektoratet

> ***Data and AI are the ingredients for innovation*** *that can help us to find solutions to societal challenges, from health to farming, from security to manufacturing. In order to release that potential we have to find our* ***European way, balancing the flow and wide use of data while preserving high privacy, security, safety and ethical standards****.*

Ursula von der Leyen, European Commission President
“A Union that strives for more - My agenda for Europe” (2019)

Digdir

digdir.no

Data Sharing and Data Economy Timeline

PSI/ODD Directive
(EU) 2019/1024

2019

2020

Data Governance Act

Artificial Intelligence
Act (AIA)

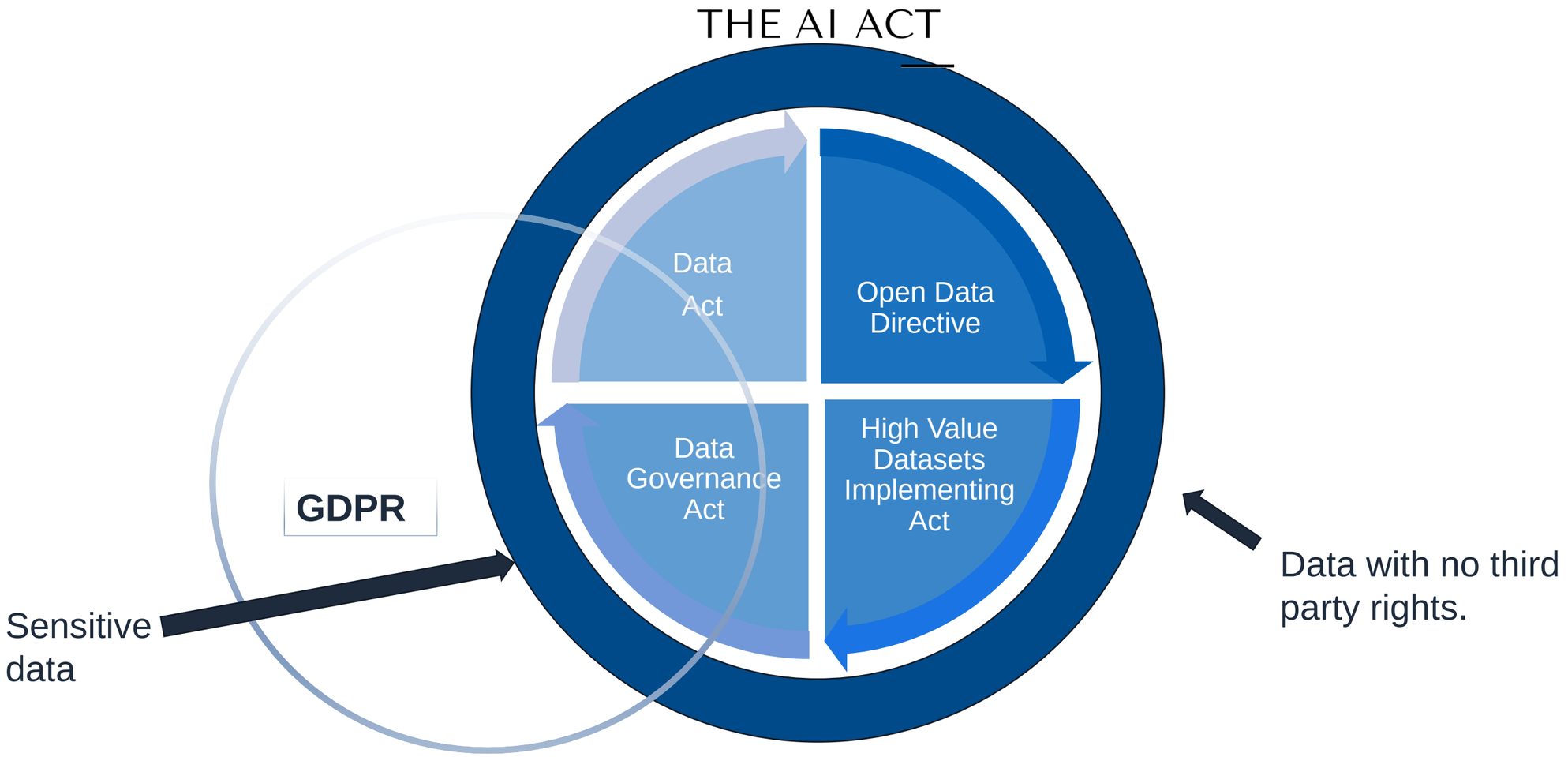
2021

2022

Data Act

HVDs Implementing Act

EU regulation on sharing and use of data



Why?

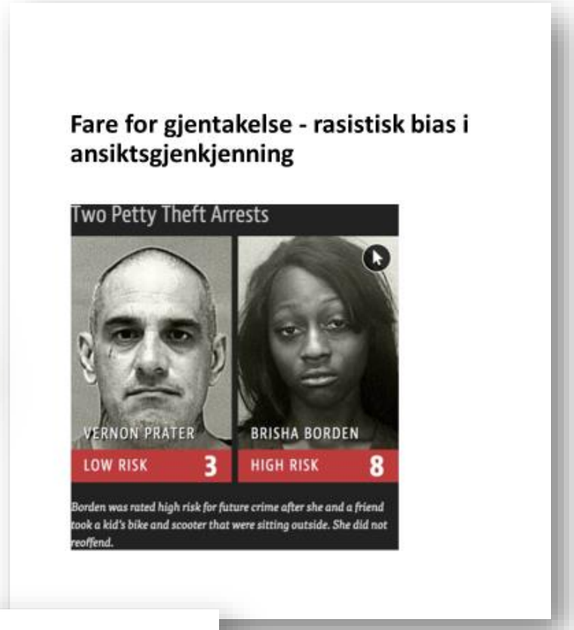
1. Avoid fragmentation

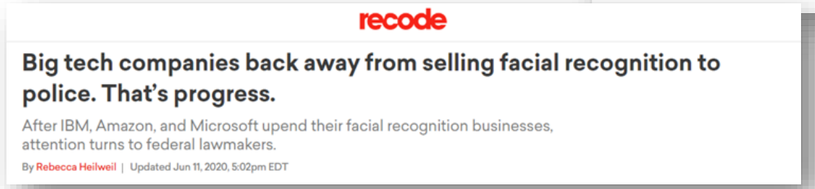
A **Common European Approach to AI is necessary** to reach sufficient scale and **avoid the fragmentation** of the single market.

Why?

1. Avoid fragmentation
2. Build trust

THE AI ACT





Why?

1. Avoid fragmentation
2. Build trust
3. First mover

The EU enjoys a first mover advantage, in that, to its knowledge (as stated publicly), no other political entity in the world has proposed a legal system to regulate it.

Current definition

‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

What? Techniques and Approaches

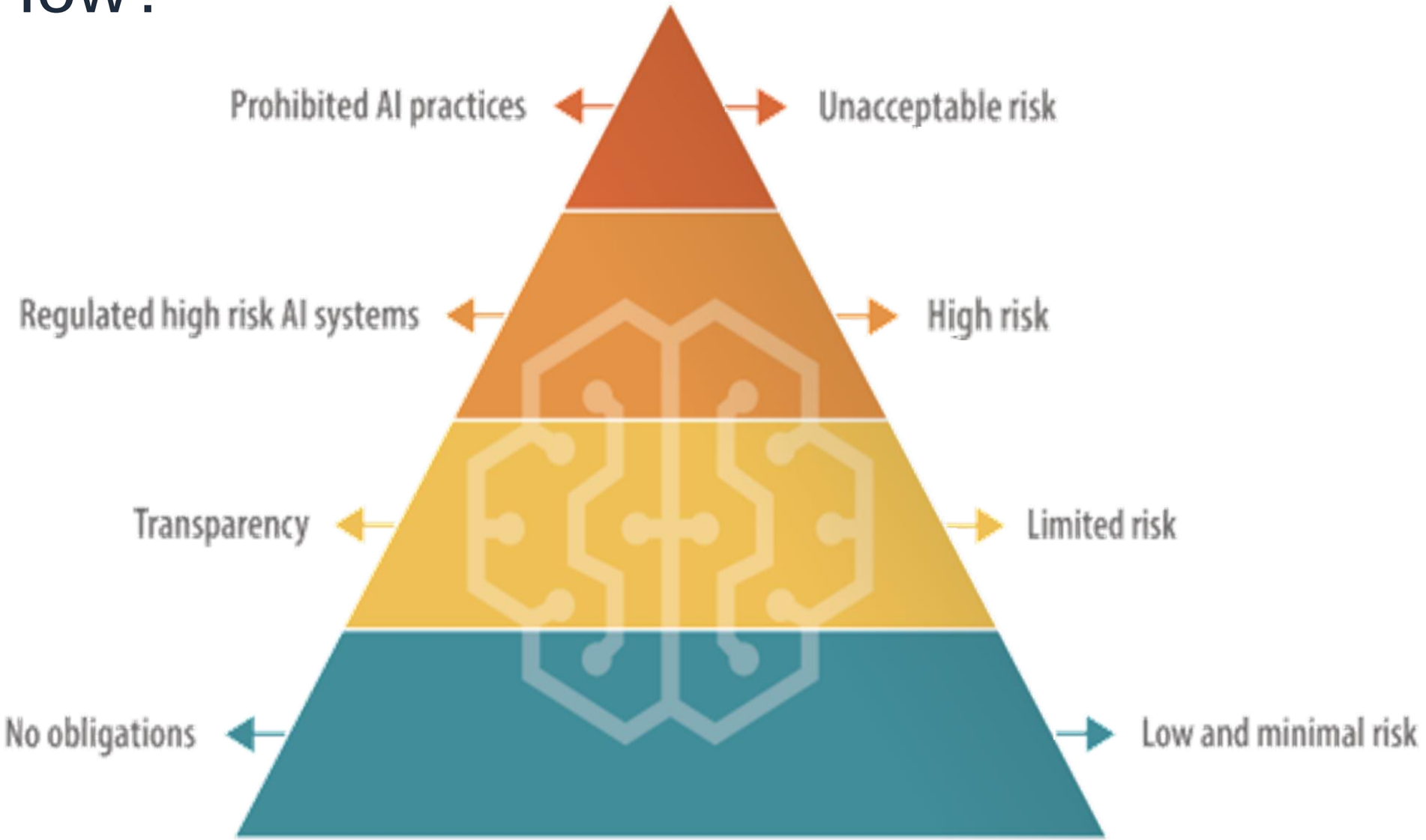
(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

How?

THE AI ACT



THE AI ACT

Unacceptable = Prohibited

- Subliminal techniques to manipulate a person's behavior
- Exploits vulnerabilities of any group
- "social credit scoring;"
- Real-time remote biometric identification in publicly accessible spaces by law enforcement except in certain time-limited public safety scenarios.

THE AI ACT

- Limited risk (chatbots etc.)
  - Minimal transparency obligations.
- Minimal risk (Majority of AI)
  - Free use of applications such as AI-enabled video games or spam filters.

THE AI ACT

- Critical infrastructures (e.g. transport), that could put the life and health of citizens at risk
- Educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams)
- Safety components of products (e.g. AI application in robot-assisted surgery)
- Employment, workers management and access to self-employment (e.g. CV sorting software for recruitment procedures)
- Essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan)
- Law enforcement that may interfere with people's fundamenta evaluation of the reliability of evidence)
- Migration, asylum and border control management (e.g. verifi authenticity of travel documents)
- Administration of justice and democratic processes (e.g. appl concrete set of facts)

Estimated that 15% of all AI systems will be high risk

Many public sector services will end up as high risk!

Rules for High Risk

- Conduct conformity assessment
- File System in newly established EU-wide database for high-risk AI systems.

THE AI ACT

Technical and Auditing Requirements for High-Risk AI

- Risk management system for the entire lifecycle of the system
- Testing the system to identify risks and determine appropriate mitigation measures
- Validate that the system runs consistently for the intended purpose
- data governance controls, including the requirement that all training, validation, and testing datasets be complete, error-free, and representative;
- Detailed technical documentation, including around system architecture, algorithmic design, and model specifications;
- Automatic logging of events while the system is running, with the recording conforming to recognized standards;
- Sufficient transparency to allow users to interpret the system’s output;
- Designed to maintain human oversight at all times

Åpne data-direktivet (ODD)

- «Innebygd åpenhet og åpenhet som standardinnstilling".

- Direktivet et minimumsdirektiv med formål om å fremme viderebruk av offentlig informasjon. Det skal styrke EUs dataøkonomi ved å øke tilgjengeligheten av offentlige og offentlig finansierte data.

- Direktivet etablerer særregler for såkalte datasett med høy verdi og for dynamiske data.

- Flere av endringene i det nye åpne-data direktivet følger allerede av offentleglova med forskrift. Det er likevel behov for justeringer i regelverket da åpne data-direktivet har etablert enkelte særregler for noen typer dokumenter (data), eksempelvis forskningsdata.

Direktivet har som mål å styrke EUs dataøkonomi

- redusere markedsadgangsbarrierer, særlig for små og mellomstore bedrifter
- øke tilgjengeligheten av data
- minimere risikoen for overdrevne fordeler ved å være først på markedet (*first-mover advantage*),
- øke forretningsmulighetene

Dynamiske data og høyverdi datasett

- **Dynamiske data:** dokumenter i digital form som oppdateres hyppig eller i sanntid, særlig på grunn av deres volatilitet, eller at de raskt foreldes
- **Høyverdi datasett**: dokument/data hvis gjenbruk kan gi viktige fordeler for samfunnet, miljøet og økonomien

Kommisjonen vedtar implementing act (gjennomføringsrettsakt) som **fastslår en liste av spesifikke høyverdi datasett**

Slike spesifikke høy-verdi datasett **skal være:**

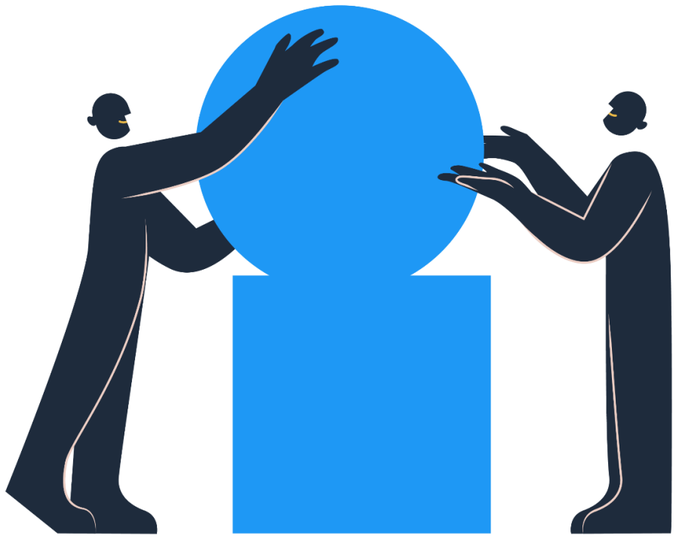
a. Tilgjengelige gratis
b. Maskinlesbare
c. Tilbudt via APIer
d. Tilbys for bulk download (komplett nedlasting) der det er relevant.

Identifiseringen av spesielle høyverdi datasett skal baseres på en vurdering av potensialet for å

a. Generere signifikante sosioøkonomiske og miljømessige gevinster og innovative tjenester.
b. Være til nytte for et høyt antall brukere, særlig SMBs.
c. Bidra til å generere verdi (generate revenues).
d. Kombineres med andre datasett.

Kategorier høyverdi datasett:

- Geografiske data
- Jordobservasjonsdata og miljødata
- Meteorologiske data
- Statistikk
- Selskapsregister og eierskapsregister
- Mobilitetsdata (transportdata)



Datastyringsforordningen (DGA)

- Mer og lettere tilgang til europeiske data.
- Rammeverk for trygg gjenbruk av beskyttede data fra offentlig sektor.

- **Dataformidlere -** disse skal tilby trygge måter for firmaer og personer å dele beskyttede data på, som sikrer at dataene gjenbrukes i tråd med regelverket de er underlagt.
- **Dataaltruisme -** medlemsstatene **kan** etablere organisatoriske og/eller tekniske ordninger som legger til rette for datalatruisme.
- **European Data Innovation Board -** Skal rådgi Kommisjonen om blant annet helhetlig praktisering av regelverket og hvordan man kan sikre interoperabilitet mellom dataformidlere.
- Både offentlige virksomheter og dataformidlere får begrenset mulighet for å ta betalt for visse typer tjenester/infrastruktur.

Noen roller som følger av DGA:

Gjennom datastyringsforordningen (data governance act, DGA) pålegges Norge og EUs medlemsland å opprette en del nye roller og funksjoner. Samtlige kan legges til nye eller eksisterende virksomheter.

- Single information point
- Competent body/bodies
- Competent authorities

Takk for oppmerksomheten!

Spørsmål?

ressurssenteret@digdir.no

digdir.no

Digitaliseringsdirektoratet
postmottak@digdir.no
22 45 10 00
Postboks 1382 Vika, 0114 Oslo

Besøksadresser:
Industriveien 1, 8900 Brønnøysund
Skrivarevegen 2, 6863 Leikanger
Grev Wedels Plass 9, 0151 Oslo