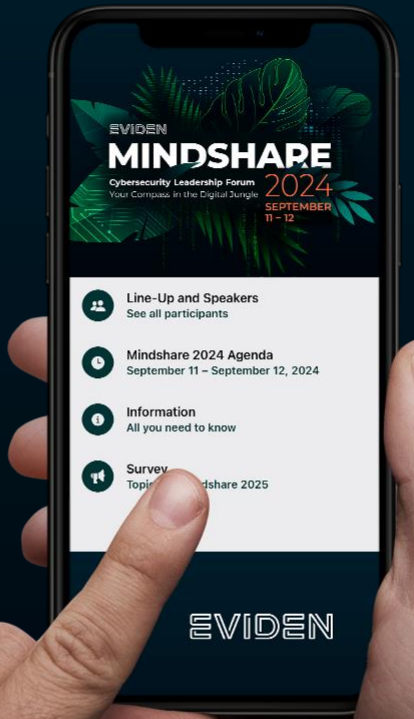
MINDSHARE 2024 AGENDA

SCAN NOW !



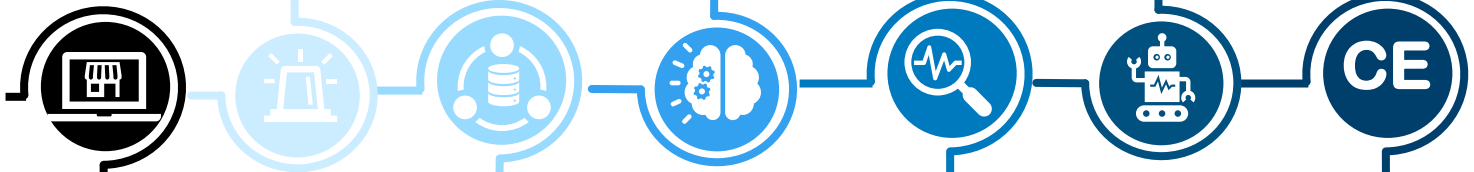
EVIDEN

Digital regulation in the EU : A critical overview

Encryption and digital signatures explained

Marina Bojarski, EVIDEN

EVIDEN MINDSHARE 2024



2023

Digital Markets Act

- New set of obligation for « gatekeepers » (more than 6,5B€ of revenues over the last 3 years and large base of users

2023

2023

Digital Services Act

- Modernisation of digital services with a focus on illicit content regulations and transparency

2022

Data Governance Act

- Rules for Data spaces and especially with obligations of independence of intermediaries
- European framework for public data access
- Concept of data altruism

2024

AI Act

- Risk based approach of AIs
- Obligation for high-risk AI
- Prohibition of blacklisted Ais
- Obligations for General-purpose AI

2024

Data Act

- Access to data from any data-generating products and related services
- Cloud providers switching
- Interoperability & smart contracts standardization

202?

AI liability directive

- Liability throughout the life of the high-risk AI system for any damage (discrimination comprised)
- Presumption of causal link in the case of fault
- Disclosure of evidence to identify the fault origin

2024

Cyber Resilience Act

- Obligations for manufacturer depending on risk class (e.g. 3rd party risk assessment)
- Declaration of conformity
- Report to ENISA within 24h of becoming aware of an attack
- Responsibility of the manufacturer

Artificial Intelligence: From global principles to practical actions

2019 - OECD AI

- Setting up the international AI principles

2021 - EUAI Act

- First AI regulation
- Based on a risk approach

2022 - US Proposal for Algorithmic Accountability Act

- Impact assessments for automated decision systems deployed for a set of critical decisions

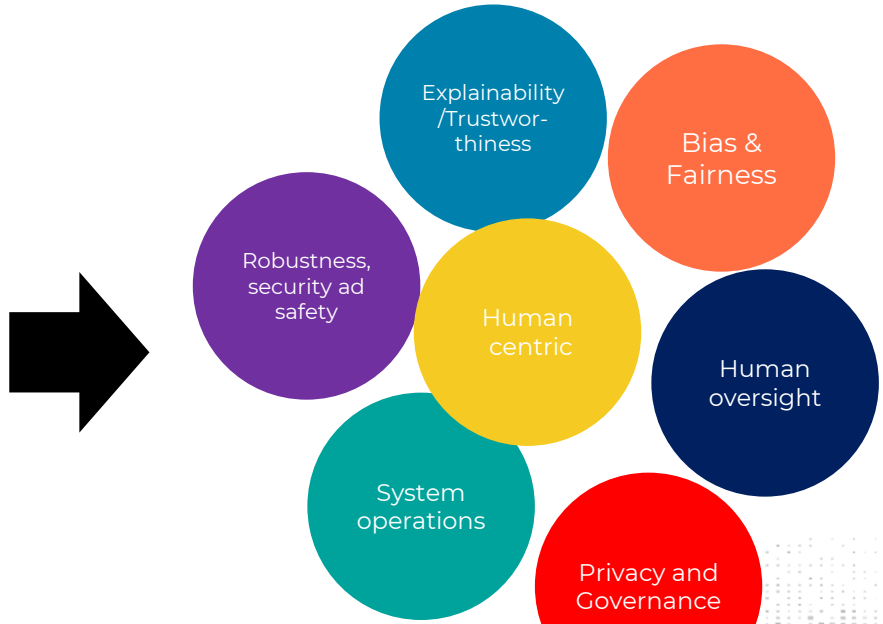
2023 - US Blue Print for AI Bill of Rights

- Principles and associated practices to help guide the design, use, and deployment of automated systems

2023 – US Executive Order on safe, secure, and trustworthy artificial intelligence

- Standards for AI safety and security, protects Americans' privacy, advances equity and civil rights, stands up for consumers and workers

2023 - The Bletchley Declaration of the AI Safety Summit



AI Act Overview

Definition of AI System

An AI is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Prohibited AI

Prohibition of:
- Social credit scoring
- Emotion recognition
- AI exploiting people's vulnerabilities
- Untargeted scraping of facial images for facial recognition
- Biometric categorisation systems
- Predictive policing
- Law enforcement use of real-time biometric in public (apart from limited pre-authorised situations

High-risk AI

- Safety components of regulated products (e.g. machinery, medical devices, aviation, …)
- Certain stand-alone AI systems (e.g. critical infrastructures, employment, law enforcement, …)

Strict obligations before entering the market:
- Notification obligation;
- Adequate risk assessment and mitigation systems;
- Fundamental rights impact assessment;
- Logging of activity to ensure traceability of results;
- Instruction of use for downstream deployers;
- Detailed documentation for authorities to assess its compliance;
- Clear and adequate information to the user;
- Appropriate human oversight measures to minimize risk;
- High level of robustness, security and accuracy.

No unfair contractual terms unilaterally imposed on an SME or startup

Limited-risk AI

Transparency obligation
Notification of users that they are interacting with a machine

Low-risk AI

No specific obligation

List of High-risk AI systems

High-risk AI

Safety components of regulated products

Machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway, installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices

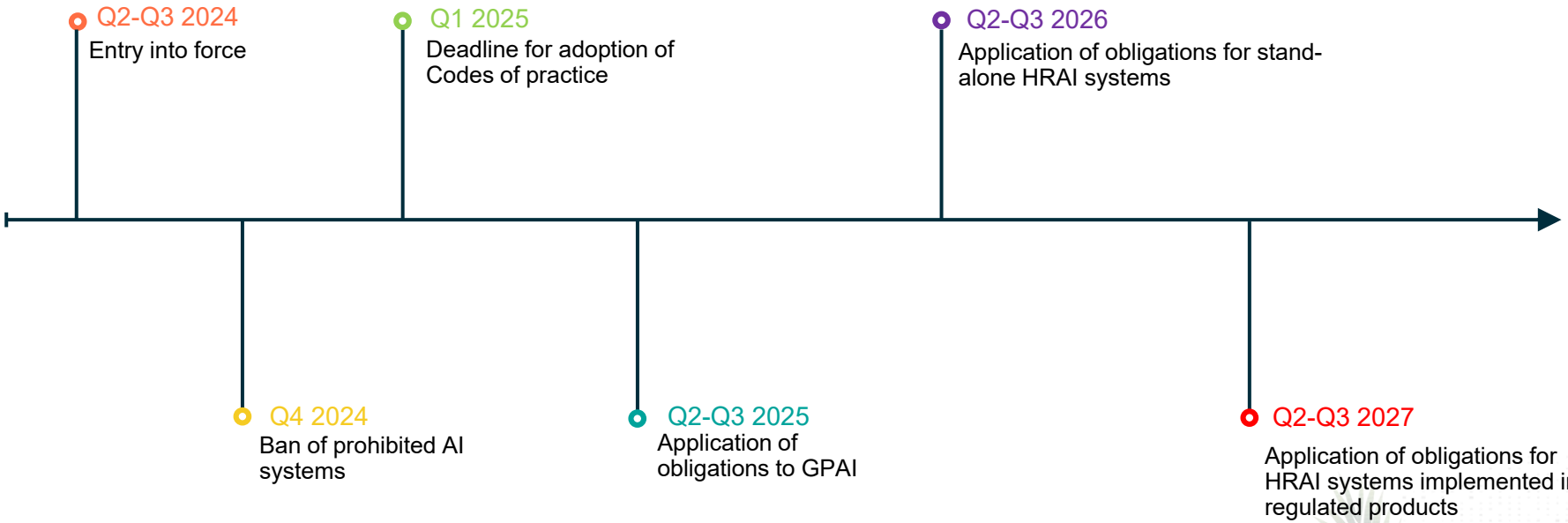
Stand alone AI systems touching on certain fundamental rights

- **Biometrics** (biometric verification whose sole purpose is to confirm that a specific natural person is the person he/she claims to be, …)
- **Critical infrastructure** (road traffic and the supply of water, gas, heating and electricity, …)
- **Education and vocational training** (to determine access or admission or to assign, to evaluate learning outcomes, …)
- **Employment**, workers management and access to selfemployment (targeted job advertisements, to analyse and filter job applications, and to evaluate candidates, …)
- **Access to and enjoyment of essential private or public services and benefits** (evaluate the eligibility for essential public assistance benefits and services, evaluate the creditworthiness, evaluate and classify emergency calls, …)
- **Law enforcement** (risk assessment of an individual, profiling or assessing the risk of a natural person of offending or re-offending, …)
- **Migration, asylum and border control management** (assess risk of irregular migration, eligibility assessment for status, detection, recognition or identification)
- **Administration of justice and democratic processes** (researching and interpreting facts, influencing the outcome of an election, …)

Unless it

- Performs narrow procedural tasks
- Improves results of a previously completed human decision
- Detects decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review
- Performs a preparatory task to an assessment relevant for the purpose of the use cases listed

AI Act timeline & sanctions



Sanctions – from 1,5% to 7% of global annual turnover (or 7,5M€ to 35M€ depending on the violation)

Key highlights of the DSA and DMA

Digital Market Act

- **Regulates « gatekeepers"** (large digital platforms) to ensure fair competition by preventing abuse of market power.
- **Imposes obligations** like allowing interoperability, transparency in advertising, and data sharing with business users.
- **Prohibits unfair practices**, such as self-preferencing, restricting third-party access, and misusing data from business users.

Digital Services Act

- **Content and user protections**: Platforms must remove illegal content swiftly, respect user rights (including appeals), and provide transparent moderation processes.
- **Transparency and accountability**: Platforms must disclose how algorithms and ads work, with strict rules for very large platforms (VLOPs) to assess societal risks.

From Data Silos to Data Lakes

Data silos

- Limited data accessibility across organizations.
- Redundancy and inefficiencies due to duplicated data.
- Hinders comprehensive data analysis and innovation.

Data lakes

- Facilitates cross-sector and cross-border data exchange in line with the EU's Digital Strategy.
- Enables advanced analytics, AI, and machine learning by aggregating large volumes of diverse data.
- Drives innovation and operational efficiency by breaking down barriers between departments and organizations.

EU regulation promoting data openness

Data Act

- **Data Transparency**: Requires federal agencies to standardize and publicly disclose spending and performance data.
- **Data Management**: Mandates practices for improving data accessibility and usability.
- **Data Quality**: Sets standards for data accuracy and consistency.
- **IoT Data**: Promotes integration and standardization of data from IoT devices.

Data Governance Act

- **Facilitates Secure Data Sharing**: Establishes frameworks for safe and trustworthy data sharing across sectors and borders within the EU.
- **Empowers Data Intermediaries & Altruism**: Introduces neutral intermediaries and allows voluntary data sharing for public good (e.g., research, public services).
- **Enhances Public Sector Data Reuse**: Allows the reuse of sensitive public sector data while ensuring data protection and security standards.

Questions?

Marina Bojarski, EVIDEN

TAKE A MINUTE AND GIVE US FEEDBACK …

RATE NOW!