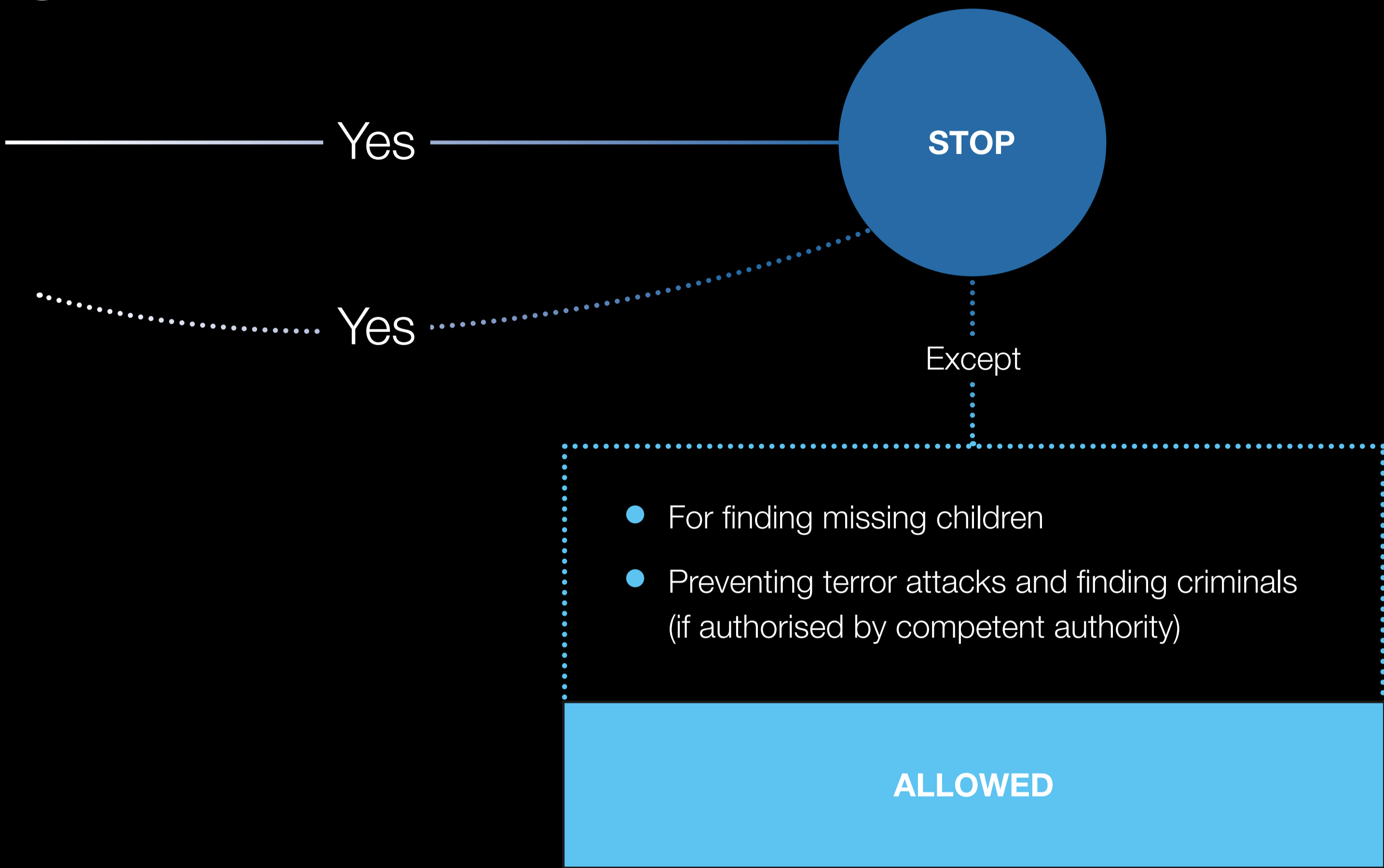


AI System

Prohibited use?

- Manipulates behaviour
- Exploits vulnerabilities
- Social scoring by the government
- Remote biometric identification in publicly accessible spaces for law enforcement

No



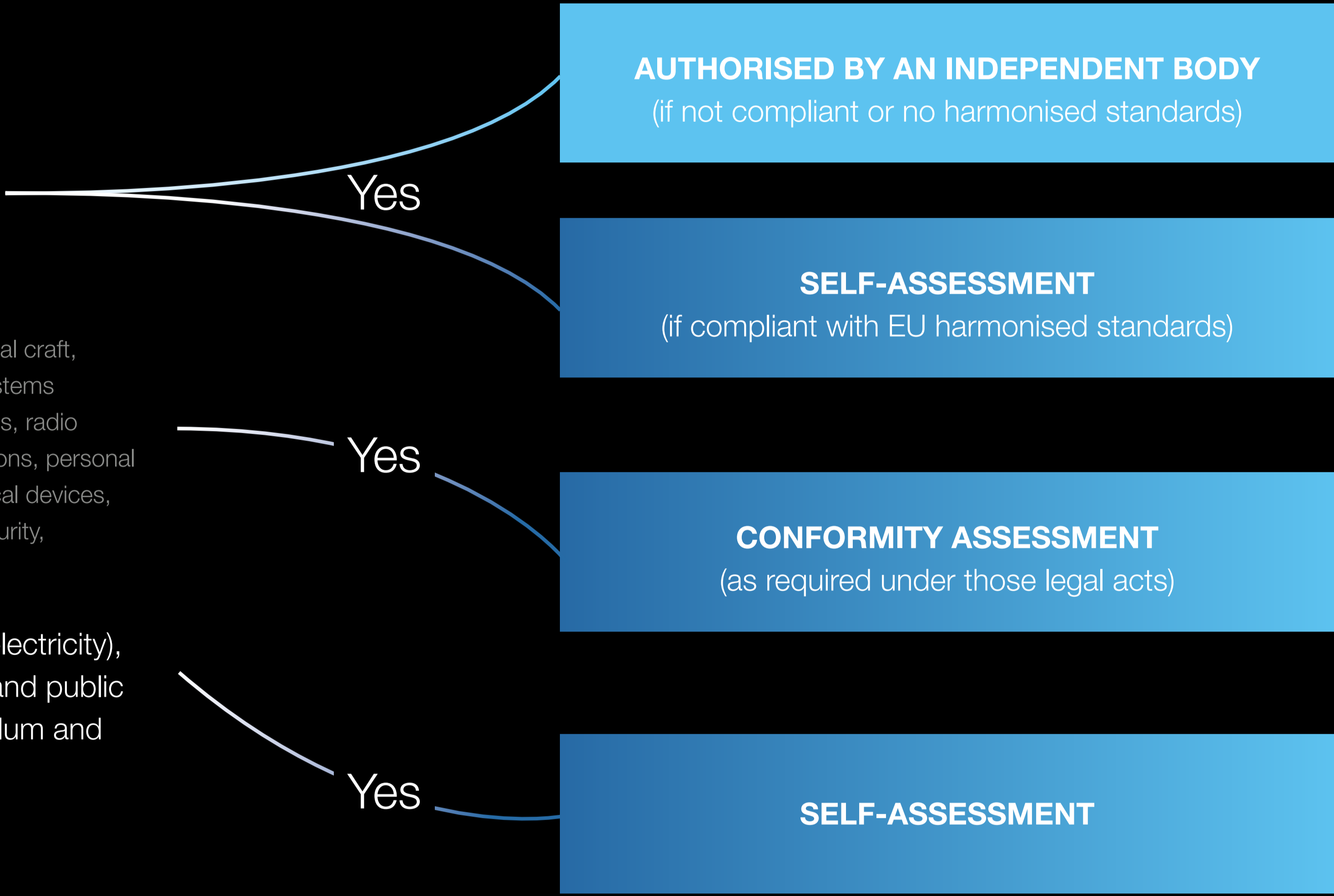
High risk?

Requirements for all high-risk AI Systems:

- High-quality data
- Logging of activity to ensure traceability of results
- Documentation and record keeping for verification
- Transparency of information to users
- Human oversight
- Robustness, accuracy and security

- Remote biometric identification
- Safety components of products covered by existing legislation
(including credit scoring, machinery, toys, recreational craft, elevator components, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, cableway installations, personal protective equipment, burning gaseous fuels, medical devices, in vitro diagnostic medical devices, civil aviation security, vehicles, marine equipment, rail systems)
- Critical infrastructure (roads, water, gas, electricity), education, recruitment, essential private and public services, law enforcement, migration (asylum and border control), administration of justice

No



Limited risk?

- Interacts with humans
(eg. Chatbots)
- Detects emotions or determines association with (social) categories based on biometric data
- Generates or manipulates content ('deep fakes')

No



Minimal risk?

- All other uses
(eg. video games, AI-based spam filters, language processing, data centers energy use adjustment, screen brightness adjustments etc)

