

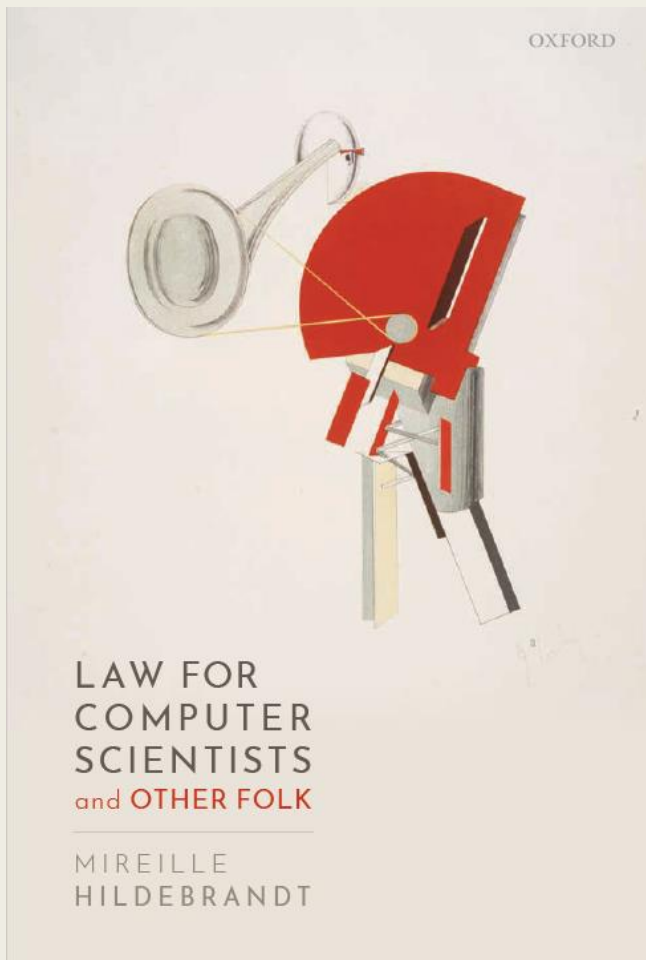


AI ACT AND TAILORED AI-SYSTEMS

© GR STOCKS

OPEN ACCESS at OUP

- First ever comprehensive textbook
- Based on 8 years of teaching law to master students of computer science
- Systematic introduction of what law ‘does’
- Dedicated chapters highly relevant for CS: e.g. cybercrime, data protection, copyright
- A dive into future scenarios:
 - Legal protection by design
 - Legal personhood for AI systems?



What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

What's Up?

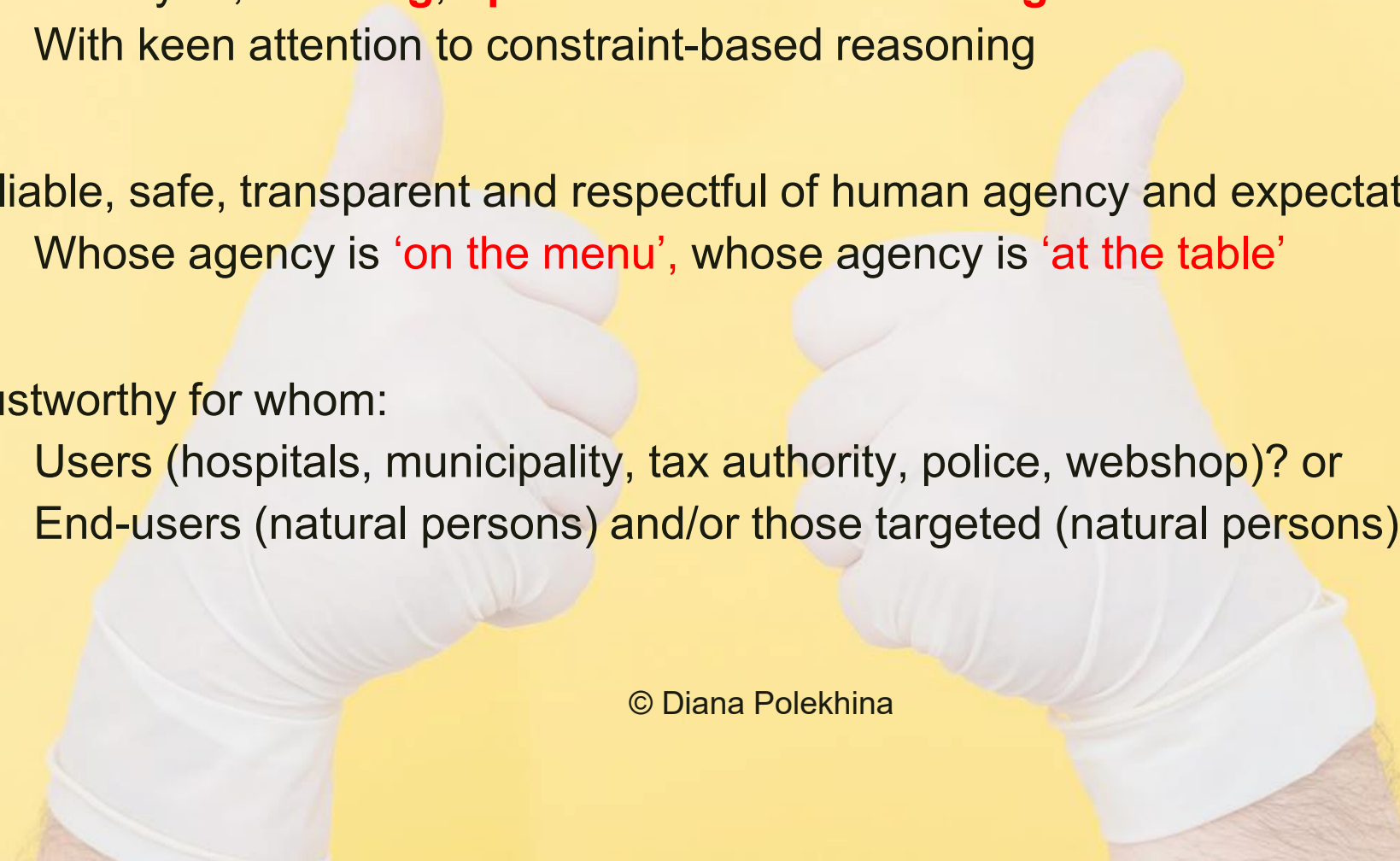
- **Tailoring**
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'



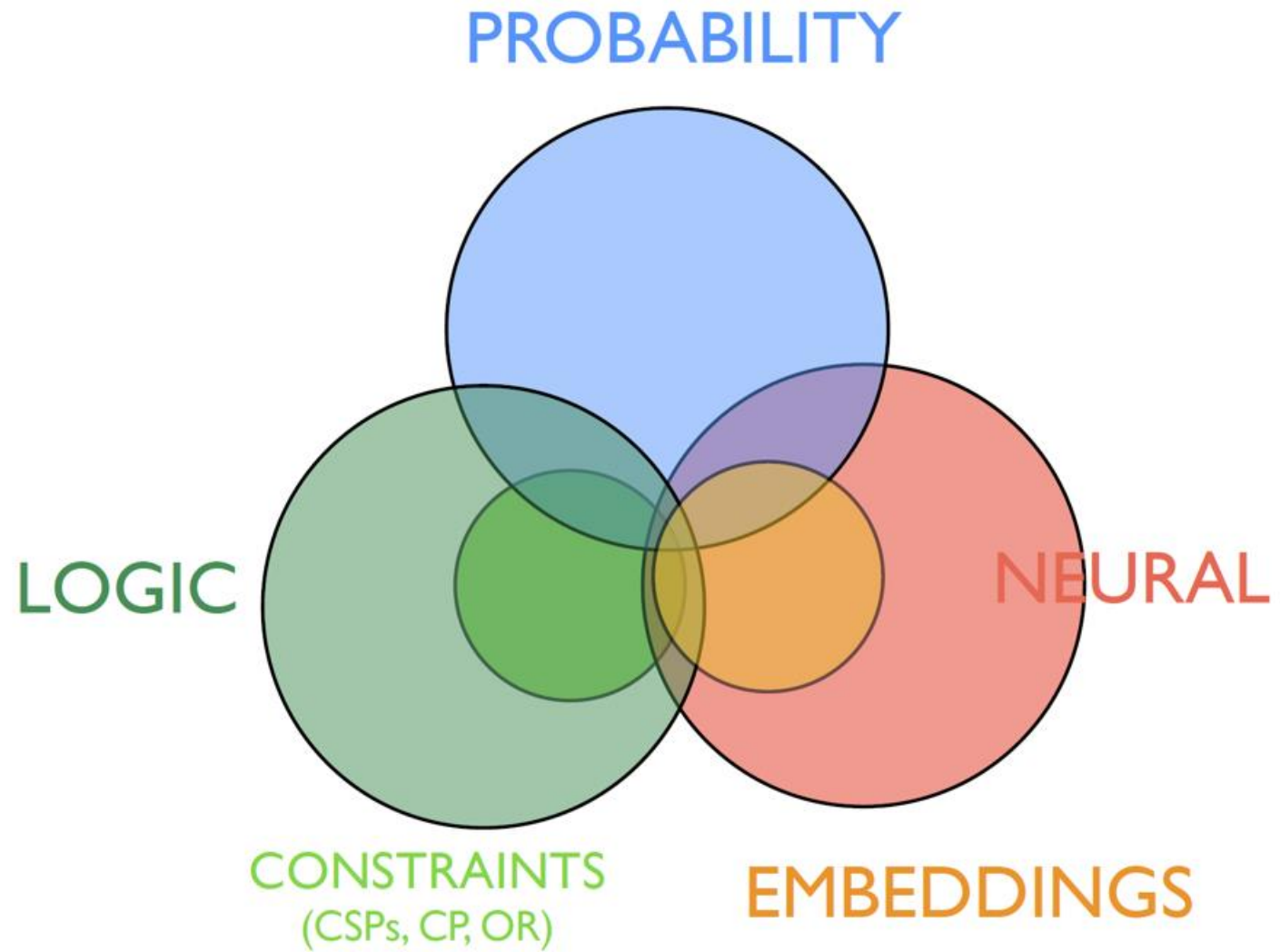
Fosca Gianotti:

- We want to build not intelligent machines
 - But machines that make human more intelligent

© James Lee

- 
- Trustworthy AI, **learning, optimisation** and **reasoning**: TAILOR
 - With keen attention to constraint-based reasoning
 - Reliable, safe, transparent and respectful of human agency and expectations
 - Whose agency is **'on the menu'**, whose agency is **'at the table'**
 - Trustworthy for whom:
 - Users (hospitals, municipality, tax authority, police, webshop)? or
 - End-users (natural persons) and/or those targeted (natural persons)?

© Diana Polekhina



Defining AI system

- Annex 1:
 - 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.

Defining AI system

- Definition of AI system in art. 3(1):
 - 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;

Defining AI system

- Definition has a **broad scope** and is meant to provide **broad protection**
- It is not about what AI truly is (no metaphysical discussions)
- Meant to provide **'effective and practical protection'**
- The discussion should be about:
 - whether **the right level of protection** has been implemented
 - depending on the qualification as prohibited, high risk or other

TAILOR on acting

How does an AI agent decide and learn on how to act?

- empowering the agent with the ability of deliberating autonomously how to act in the world.
 - reasoning on the effects of its actions,
 - learning from past experiences (or simulation of experiences), as well as
 - monitoring the actual outcome of its actions,
 - learning possibly unexpected outcomes, and again
 - reasoning and learning how to deal with such new outcomes.
- This carries **significant risks** and therefore we must be able to balance such power with safety. This means that the autonomy of the agent must be guarded by human guided specifications and oversight, to make it verifiable and comprehensible in human terms and ultimately trustworthy.

TAILOR on social

How do AI agents act and learn in a society?

- How do we empower **individual AI agents to communicate with each other**, collaborate, negotiate and reach agreements? How can agents coordinate to fairly share common resources?
- How can we **make agents learn from each other** in a responsible and fair way, leading to more intelligent behavior?
- How to create **trustworthy hybrid human-AI societies** that fulfil humans' expectations and follow their requirements?"

TAILOR on auto AI

How can we use AI “at the meta-level” to ensure that AI tools and systems are performant, robust and trustworthy, especially when built, deployed, maintained and monitored by people with limited AI expertise?

- AutoAI: to diligently **automate the labor-intensive and error-prone aspects** of building AI systems to make them more trustworthy and robust
- ***AutoML in the Wild. Beyond standard supervised learning. Self-monitoring AI Systems. Multi-objective AutoAI. Ever-learning AutoAI.***

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

According to the Guidelines, trustworthy AI should be:

(1) **lawful** - respecting all applicable laws and regulations

(2) **ethical** - respecting ethical principles and values

(3) **robust** - both from a technical perspective while taking into account its social environment

7 key requirements: mapping against AI Act

1. Human agency and oversight –

- art. 14 (human oversight)

2. Technical Robustness and safety –

- art. 9 (risk management system),
- Art. 15 (accuracy, robustness and cybersecurity)
- Art. 17 (quality management system)

7 key requirements: mapping against AI Act

3. Privacy and data governance

- Art. 7, 8 Charter and GDPR
- Art. 10 AI Act (data and data governance)

4. Transparency

- Art. 11 and 12 (technical documentation and recordkeeping)
- Art. 13 (transparency and provision of information to users)
- Art. 52 (transparency for emotion recognition, biometric categorisation, deepfakes and all systems that interact with humans)
- ...

7 key requirements: mapping against AI Act

5. Diversity, non-discrimination and fairness

- Art. 10 (data and data governance): 2(f) (check for bias) and 5 (exception prohibition of processing sensitive data)
- **Art. 15 (accuracy, robustness and cybersecurity): 3 (feedback loops that reinforce bias)**

6. Societal and environmental well-being:

- Art. 69 (codes of conduct): voluntary application of AI systems for requirements related to environmental sustainability

7 key requirements: mapping against AI Act

7. Accountability:

- Title III: Chapter 5 (standards, conformity assessment, certificates, registration)
- Title X: art. 71 (penalties): up to 30 million euro or 6% global turnover; or up to 20 million euro or 4% global turnover; or up to 10 million euro or 2% global turnover
- Accountability in the AI Act falls upon
 - providers and users
 - and distributors and importers

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- **Architecture of the Act**
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues

Overall Goals AI Act

- High risk AI systems:
 - Protection against **safety and health risks** (Annex II)
 - Protection against infringements of **fundamental rights** (Annex III)
- **Requirements for high risk systems:**
 - Title III, chapters 2, 3
 - Risk management, Quality management, Data and data governance, Human oversight, Technical documentation, Record keeping, Transparency for users, Accuracy, robustness and cybersecurity

Compliance in case of high risk AI systems

EU declaration of conformity (Art. 48)

1. The provider shall draw up a written EU declaration of conformity for each AI system and keep it at the disposal of the national competent authorities for 10 years after the AI system has been placed on the market or put into service.

The EU declaration of conformity shall identify the AI system for which it has been drawn up. A copy of the EU declaration of conformity shall be given to the relevant national competent authorities upon request.

The EU declaration of conformity shall state that the high-risk AI system in question meets the requirements set out in Chapter 2 of this Title. The EU declaration of conformity shall contain the information set out in Annex V and shall be translated into an official Union language or languages required by the Member State(s) in which the high-risk AI system is made available.

Enforcement

Steep fines when violating the requirements:

- Up to 30.000.000 Euro or 6% of global turnover
 - in case of violation of the **prohibition of certain AI practices** in art. 5
 - In case of violation of the **requirements of data and data governance** in art. 10
- Up to 20.000.000 euro or 4% of global turnover
 - In case of **all other violations of the AIA**
- Up to 10.000.000 euro or 2% of global turnover
 - In case of **incorrect, incomplete or misleading information** to notified bodies and national competent authorities in reply to a request

Architecture of the Act

- **Applicable to**
 - AI systems (broad definition)
 - AI practices (narrowly defined)
- **Addressing providers, distributors, importers:**
 - Putting on the market (first making available on the market)
 - Making available on the market
- **Addressing users:**
 - Putting into service (first use)
 - Using
- **Prohibitions of 4 AI practices**
- **Requirements for high risk AI systems**
- **Transparency for 4 types of AI systems**
- **Post market monitoring**

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

Roles

Those addressed by the Act

- Provider: entity that **develops or has others develop** and AI system with a view to **placing it on the market or putting it into service under its own name or trademark**, whether for payment or free of charge
- User: **using an AI system under its authority**, except where the AI system is used in the course of a **personal non-professional activity**
 - Also: importer, distributor, etc.

Layered approach

■ Prohibition AI practices:

- Manipulation or exploitation of vulnerable groups or individuals, social credit scoring by governments, remote real time biometric identification by police (with exceptions)

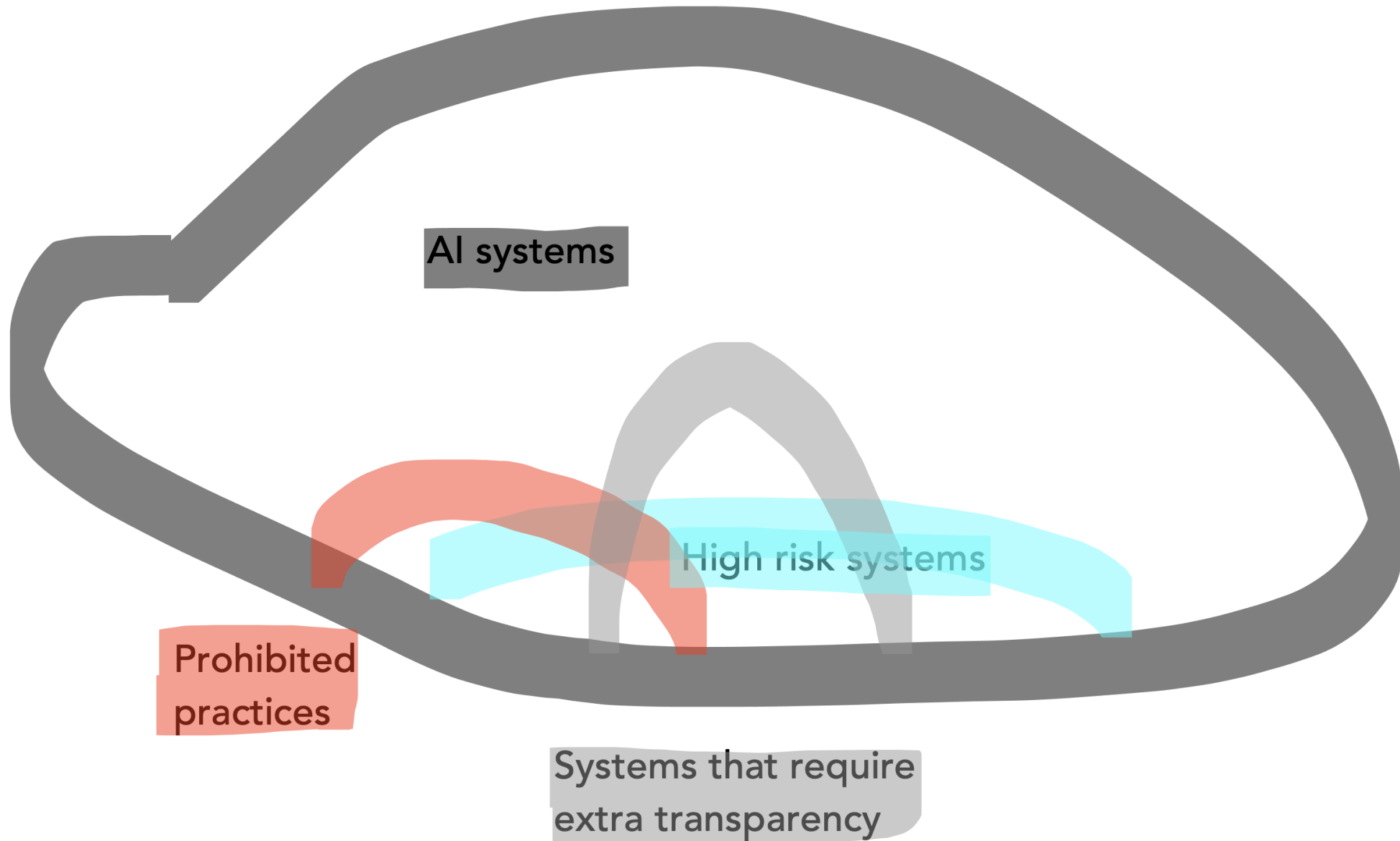
■ High risk AI systems

- Products or **safety** components of products regulated in Annex II
- Standalone AI systems as defined in Annex III (focused on **fundamental rights**)

■ Transparency requirements for certain AI systems

- Systems interacting with natural persons
- Emotion recognition systems
- Biometric categorisation systems
- Systems producing deepfakes

- An AI system may be high risk and nevertheless prohibited, if part of a prohibited practice
- An AI system may be due to special transparency requirements and also be high risk or even prohibited



What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

Requirements for high risk AI systems

Risk management system (Art. 9)

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems

Requirements for high risk AI systems

Risk management system (Art. 9)

2. The risk management system shall consist of
 - a **continuous iterative process**
 - run throughout the **entire lifecycle** of a high-risk AI system,
 - requiring **regular systematic updating**.
 - It shall comprise the following steps:

Requirements for high risk AI systems

Risk management system (Art. 9)

2. It shall comprise the following steps:
 - a. **identification and analysis** of the **known and foreseeable risks** associated with each high-risk AI system;
 - b. **estimation and evaluation** of the risks that may emerge when the high-risk AI system is used in accordance with its **intended purpose** and under conditions of **reasonably foreseeable misuse**;
 - c. **evaluation of other possibly arising risks** based on the analysis of data gathered from the **post-market monitoring system** referred to in Article 61;
 - d. **adoption of suitable risk management measures** in accordance with the provisions of the following paragraphs.

Requirements for high risk AI systems

Risk management system (Art. 9)

3. The risk management measures referred to in paragraph 2, point (d)
 - shall give due consideration to the **effects and possible interactions**
 - resulting from the combined application of the requirements set out in this Chapter 2.
 - They shall take into account **the generally acknowledged state of the art**,
 - including as reflected in relevant harmonised standards or common specifications.

Requirements for high risk AI systems

Risk management system (Art. 9)

4. The risk management measures referred to in paragraph 2, point (d)
 - shall be such that **any residual risk associated with each hazard**
 - as well as the **overall residual risk of the high-risk AI systems**
 - is judged **acceptable**,
 - provided that the high-risk AI system is **used in accordance with its intended purpose**
 - or under conditions of **reasonably foreseeable misuse**.
 - **Those residual risks shall be communicated to the user.**

Requirements for high risk AI systems

Risk management system (Art. 9)

4. In identifying the most appropriate risk management measures, the following shall be ensured:
- a) **elimination or reduction of risks as far as possible through adequate design and development;**
 - b) where appropriate, implementation of **adequate mitigation and control measures** in relation to risks that cannot be eliminated;
 - c) **provision of adequate information** pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

In eliminating or reducing risks related to the use of the high-risk AI system,

- due consideration shall be given to the **technical knowledge, experience, education, training**
- to be expected by the user and
- the environment in which the system is intended to be used.

Requirements for high risk AI systems

Risk management system (Art. 9)

5. High-risk AI systems shall be tested for the purposes of
 - identifying the most appropriate risk management measures.
 - Testing shall ensure that high-risk AI systems perform consistently
 - for their intended purpose and
 - they are in compliance with the requirements set out in this Chapter.

6. Testing procedures shall be suitable to achieve the intended purpose of the AI system
 - and do not need to go beyond what is necessary to achieve that purpose.

Requirements for high risk AI systems

Risk management system (Art. 9)

7. The **testing of the high-risk AI systems** shall be performed,
 - as appropriate,
 - at **any point in time throughout the development process**, and,
 - in any event,
 - **prior to the placing on the market or the putting into service.**
- Testing shall be **made against preliminarily defined metrics**
 - and probabilistic thresholds
 - that are **appropriate to the intended purpose** of the high-risk AI system.

Requirements for high risk AI systems

Risk management system (Art. 9)

8. When implementing the risk management system described in paragraphs 1 to 7,
 - specific consideration shall be given to whether the high-risk AI system
 - **is likely to be accessed by or have an impact on children.**

9. For **credit institutions** regulated by Directive 2013/36/EU, the aspects described in paragraphs 1 to 8 shall be part of the risk management procedures established by those institutions pursuant to Article 74 of that Directive.

Requirements for high risk AI systems

Data and data governance (Art. 10)

1. High-risk AI systems

- which make use of techniques involving the **training of models with data**
- shall be developed on the basis of **training, validation and testing data sets**
- that meet the **quality criteria referred to in paragraphs 2 to 5.**

Requirements for high risk AI systems

Data and data governance (Art. 10)

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular,
 - a) the relevant **design choices**;
 - b) data **collection**;
 - c) relevant data **preparation processing operations**, such as annotation, labelling, cleaning, enrichment and aggregation;
 - d) the **formulation of relevant assumptions**, notably with respect to the information that the data are supposed to measure and represent;
 - e) a **prior assessment of the availability, quantity and suitability** of the data sets that are needed;
 - f) examination in view of **possible biases**;
 - g) the **identification of any possible data gaps or shortcomings**, and how those gaps and shortcomings can be addressed.

Requirements for high risk AI systems

Data and data governance (Art. 10)

3. Training, validation and testing data sets shall be
 - relevant, representative, free of errors and complete.
- They shall have the appropriate statistical properties,
 - including, where applicable,
 - as regards the persons or groups of persons on which the high-risk AI system is intended to be used.
- These characteristics of the data sets may be met
 - at the level of individual data sets
 - or a combination thereof.

Requirements for high risk AI systems

Data and data governance (Art. 10)

4. Training, validation and testing data sets shall take into account,
 - to the extent required by the intended purpose,
 - the characteristics or elements that are particular to
 - the **specific geographical, behavioural or functional setting**
 - within which the high-risk AI system is **intended to be used**.

Requirements for high risk AI systems

Data and data governance (Art. 10)

Article 42 Presumption of conformity with certain requirements

1. Taking into account their intended purpose,
 - high-risk AI systems that have been trained and tested
 - on data concerning the specific geographical, behavioural and functional setting
 - within which they are intended to be used
 - shall be presumed to be in compliance with the requirement set out in Article 10(4).

- CRCL paper by Sylvie Delacroix: issue of time

Requirements for high risk AI systems

Data and data governance (Art. 10)

5. To the extent that it is strictly necessary
 - for the purposes of **ensuring bias monitoring, detection and correction**
 - in relation to the high-risk AI systems,
 - the providers of such systems **may process special categories of personal data** referred to in Article 9(1) of Regulation (EU) 2016/679, Article 10 of Directive (EU) 2016/680 and Article 10(1) of Regulation (EU) 2018/1725,
 - subject to appropriate safeguards for the fundamental rights and freedoms of natural persons,
 - including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures,
 - such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

Requirements for high risk AI systems

Data and data governance (Art. 10)

6. Appropriate data governance and management practices shall apply
 - for the development of high-risk AI systems
 - other than those which make use of techniques involving the training of models
 - in order to ensure that those high-risk AI systems comply with paragraph 2.

Requirements for high risk AI systems

Human oversight (Art. 14)

1. High-risk AI systems shall be **designed and developed** in such a way,
 - including with appropriate **human-machine interface tools**,
 - that they **can be effectively overseen by natural persons**
 - during the period in which the AI system is in use.

Requirements for high risk AI systems

Human oversight (Art. 14)

2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights
 - that may emerge when a high-risk AI system is used
 - in accordance with its intended purpose or
 - under conditions of reasonably foreseeable misuse,
 - in particular when such risks persist notwithstanding
 - the application of other requirements set out in this Chapter.

Requirements for high risk AI systems

Human oversight (Art. 14)

3. Human oversight shall be ensured through either one or all of the following measures:
 - a. **identified and built**, when technically feasible, **into the high-risk AI system** by the provider before it is placed on the market or put into service;
 - b. **identified** by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate **to be implemented by the user**.

Requirements for high risk AI systems

Human oversight (Art. 14)

4. The measures referred to in paragraph 3 shall enable **the individuals to whom human oversight is assigned** to do the following, as appropriate to the circumstances:
 - a. **fully understand the capacities and limitations of the high-risk AI system** and be able to duly monitor its operation, so that **signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible**;
 - b. remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (**'automation bias'**), in particular for high-risk AI systems used to **provide information or recommendations for decisions to be taken by natural persons**;
 - c. **be able to correctly interpret the high-risk AI system's output**, taking into account in particular the characteristics of the system and the interpretation tools and methods available;
 - d. **be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system**;
 - e. be able to intervene on the operation of the high-risk AI system or interrupt the system through a **"stop" button or a similar procedure**.

Requirements for high risk AI systems

Human oversight (Art. 14)

5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 shall be such as to ensure that, in addition,
 - no action or decision is taken by the user
 - on the basis of the identification resulting from the system
 - unless this has been verified and confirmed by at least two natural persons.

Annex III

1. Biometric identification and categorisation of natural persons:
 - a. AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons;

Requirements for high risk AI systems

Accuracy, robustness and cybersecurity (Art. 15)

1. High-risk AI systems shall be **designed and developed** in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and **perform consistently** in those respects throughout their lifecycle.
2. The **levels of accuracy and the relevant accuracy metrics** of high-risk AI systems shall be declared in the accompanying instructions of use.

Requirements for high risk AI systems

Accuracy, robustness and cybersecurity (Art. 15)

3. High-risk AI systems shall be **resilient** as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems.

The **robustness** of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans.

High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations (**'feedback loops'**) are duly addressed with appropriate mitigation measures.

Requirements for high risk AI systems

Accuracy, robustness and cybersecurity (Art. 15)

4. High-risk AI systems shall be **resilient** as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.

The technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks.

The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset (**'data poisoning'**), inputs designed to cause the model to make a mistake (**'adversarial examples'**), or model flaws.

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- **Obligations for providers and users**
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

In case of high risk systems

Obligations for providers (Art. 16)

Providers of high-risk AI systems shall:

- a. ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;
- b. have a quality management system in place which complies with Article 17;
- c. draw-up the technical documentation of the high-risk AI system;
- d. when under their control, keep the logs automatically generated by their high-risk AI systems;
- e. ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its placing on the market or putting into service;

In case of high risk systems

Obligations for providers (Art. 16)

Providers of high-risk AI systems shall:

- f. comply with the registration obligations referred to in Article 51;
- g. take the necessary corrective actions, if the high-risk AI system is not in conformity with the requirements set out in Chapter 2 of this Title;
- h. inform the national competent authorities of the Member States in which they made the AI system available or put it into service and, where applicable, the notified body of the non-compliance and of any corrective actions taken;
- i. to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;
- j. upon request of a national competent authority, demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title.

In case of high risk systems

Quality management system (Art. 17)

1. Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects:
 - a. a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system;
 - b. techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system;
 - c. techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system;

In case of high risk systems

Quality management system (Art. 17)

- d. **examination, test and validation procedures** to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;
- e. **technical specifications, including standards**, to be applied and, where the relevant **harmonised standards** are not applied in full, the means to be used to ensure that the high-risk AI system complies with the requirements set out in Chapter 2 of this Title;
- f. **systems and procedures for data management**, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems;

In case of high risk systems

Quality management system (Art. 17)

- g. the **risk management system** referred to in Article 9;
- h. the setting-up, implementation and maintenance of a **post-market monitoring system**, in accordance with Article 61;
- i. procedures related to the **reporting of serious incidents and of malfunctioning** in accordance with Article 62;
- j. **the handling of communication with national competent authorities, competent authorities**, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties;

In case of high risk systems

Quality management system (Art. 17)

Article 61 Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

1. Providers shall **establish and document a post-market monitoring system** in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.
2. The post-market monitoring system shall **actively and systematically collect, document and analyse relevant data** provided by users or collected through other sources on the performance of high-risk AI systems throughout their lifetime, and allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Title III, Chapter 2.
3. The post-market monitoring system shall be **based on a post-market monitoring plan**. The post-market monitoring plan shall be part of the technical documentation referred to in Annex IV. The Commission shall adopt an implementing act laying down detailed provisions establishing a template for the post-market monitoring plan and the list of elements to be included in the plan.

In case of high risk systems

Quality management system (Art. 17)

- k. **systems and procedures for record keeping** of all relevant documentation and information;
- l. **resource management**, including security of supply related measures;
- m. **an accountability framework** setting out the responsibilities of the management and other staff with regard to all aspects listed in this paragraph.

Obligations of users of high-risk systems (Art. 29)

1. Users of high-risk AI systems shall use such systems **in accordance with the instructions of use accompanying the systems**, pursuant to paragraphs 2 and 5.
2. The obligations in paragraph 1 are **without prejudice to** other user obligations under Union or national law and to the user's discretion in organising its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider.
3. Without prejudice to paragraph 1, **to the extent the user exercises control over the input data, that user shall ensure that input data is relevant in view of the intended purpose of the high-risk AI system.**

Obligations of users of high-risk systems (Art. 29)

4. Users shall monitor the operation of the high-risk AI system on the basis of the instructions of use. **When they have reasons to consider that the use in accordance with the instructions of use may result in the AI system presenting a risk within the meaning of Article 65(1) they shall inform the provider or distributor and suspend the use of the system.** They shall also inform the provider or distributor when they have **identified any serious incident or any malfunctioning within the meaning of Article 62 and interrupt the use of the AI system.** In case the user is not able to reach the provider, Article 62 shall apply mutatis mutandis.

For users that are **credit institutions** regulated by Directive 2013/36/EU, the monitoring obligation set out in the first subparagraph shall be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Obligations of users of high-risk systems (Art. 29)

5. Users of high-risk AI systems shall **keep the logs automatically generated by that high-risk AI system**, to the extent such logs are under their control. The logs shall be kept for a period that is appropriate in the light of the intended purpose of the high-risk AI system and applicable legal obligations under Union or national law.

Users that are **credit institutions** regulated by Directive 2013/36/EU shall maintain the logs as part of the documentation concerning internal governance arrangements, processes and mechanisms pursuant to Article 74 of that Directive.

Obligations of users of high-risk systems (Art. 29)

6. Users of high-risk AI systems shall use the information provided under Article 13 to comply with their obligation to carry out a data protection impact assessment under Article 35 of Regulation (EU) 2016/679 or Article 27 of Directive (EU) 2016/680, where applicable.

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- **Connections with GDPR**
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

Connections with GDPR

- Often, 'users' of the AIA will be the 'controllers' of the GDPR
- Qualification as high risk systems:
 - under the AIA is predefined in the AIA: more legal certainty?
 - under the GDPR depends on an impact assessment (DPIA): more granular and flexible?
- Should systems qualified as high risk in Annex III require a DPIA by default?
- Compliance with AIA requirements does not imply lawfulness, this will also depend on compliance with other legislation such as GDPR (recital 41 AIA)

Connections with GDPR

- The GDPR provides for a ‘the **right to obtain human intervention** on the part of the controller, to express his or her point of view and to contest the decision’ in the case of ‘a decision based solely on **automated processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her’.
 - Only relevant for ‘decisions’
- The AIA requires that AI systems ‘shall be **designed and developed** in such a way, including with appropriate human-machine interface tools, that they can be **effectively overseen by natural persons** during the period in which the AI system is in use’.
 - Also relevant for ‘behaviour’

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- **Issues**
- 'Legal by Design' or 'Legal Protection by Design'

ISSUES

AIA = administrative law, focused on oversight bodies and administrative fines

- Upcoming legislation will settle private law liability issues
- No new individual rights are attributed to natural persons

ISSUES

I think it would help if a small set of rights were to be attributed to natural persons, while also including some collective rights:

- The right not to be subject to prohibited AI practices
- The right to object to decisions made by high-risk AI systems
- The right to file an injunction in a court of law, and to mandate that right to an NGO in case one is subjected to prohibited AI practices or to decisions made by high-risk AI systems
- The right of dedicated NGOs to file an injunction in their own name with respect to the rights under A and B

- Assuming that the upcoming AI liability framework will provide some forms of strict liability, in alignment with the product liability directive.

ISSUES

Art. 15: Accuracy, robustness, cybersecurity

- Why only accuracy?
- For individuals precision and sensitivity are far more important

ISSUES

Prohibited practices

- a, b, c require individualised harm/detriment, that is highly problematic
- the third exception of d is too broad (max. punishment of 3 years)

ISSUES

Emotion recognition and biometric categorisation

- Default: transparency requirements of art.
 - If used in contexts of ANNEX III high risk
 - If part of a prohibited practice prohibited
- Unwarranted complexity?
 - Pseudo science
- **Legal technologies are critical infrastructure, we don't want such complexity!**

What's Up?

- Tailoring
- 7 key requirements HLEG AI
- Architecture of the Act
- Roles and Layered approach
- Requirements for high risk systems
- Obligations for providers and users
- Connections with GDPR
- Issues
- 'Legal by Design' or 'Legal Protection by Design'

Constraints

- Should law be understood as part of a ‘constraint satisfaction problem’?
- Can this problem be solved with ‘constraint programming’?
- Should compliance be framed in terms of combinatorial optimisation problems?
- What would be the role for ‘operations research’ (and cybernetics, Stafford Beer 1959)?

- What’s the difference between
 - LbD (‘legal by design’) and
 - LPbD (legal protection by design)?



THE END(S)