



GWFF

GEOSPATIAL WORLD FORUM

[**CLICK TO KNOW MORE**](#)



The EU AI and Digital Services Acts and their relevance for the remote sensing industry

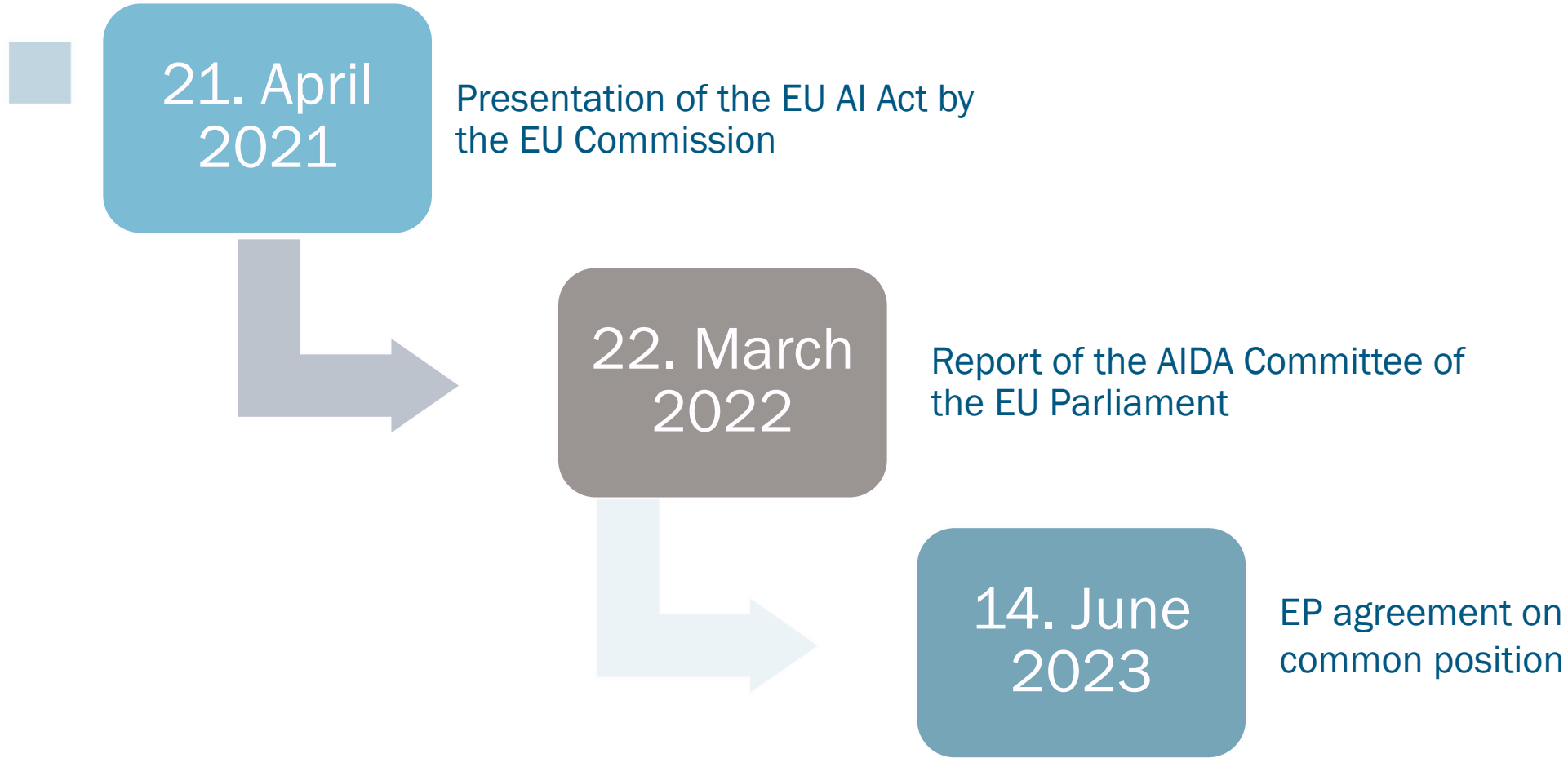
Gerhard Deiters | Attorney-at-Law/Partner at BHO Legal

GWf 2024 | Rotterdam

- I. Origin of the EU AI Act
- II. The EU AI Act
- III. Relevance of the EU AI Act for the remote sensing industry
- IV. Short introduction to the EU Digital Services Act



I. Origin of the EU AI Act



I. Origin of the AI Act

June 2023

- Start of the trialogue
- (Then) Expected completion by the end of 2024

9
November
2023

- Negotiations come to a standstill
- Headwinds from Germany, Italy and France

6 to 8
December
2023

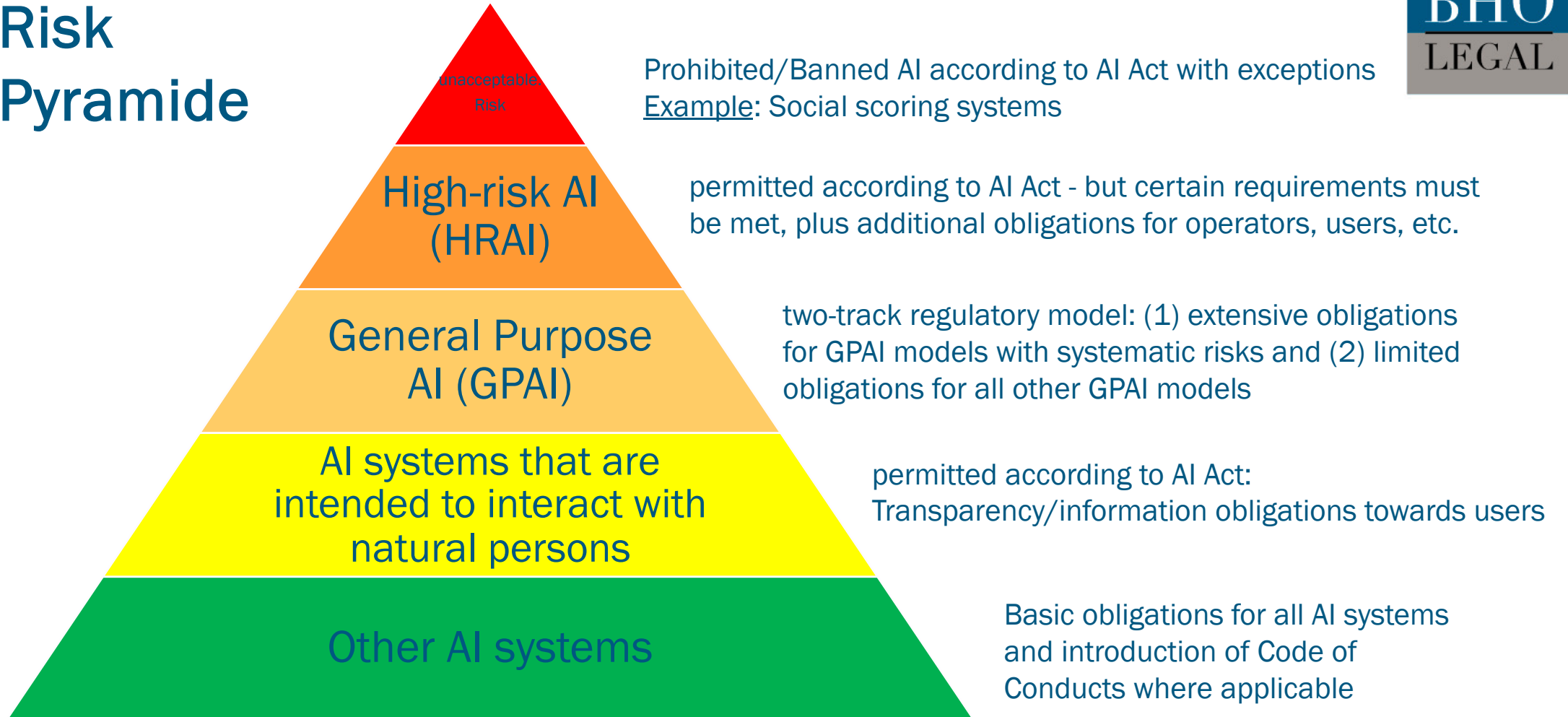
- Renewed round of negotiations
- Compromise decision

13. March
2024

- AI Act passes EP
- Expected to be published in EU journal in June 2024

II. The EU AI Act

Risk Pyramide



II. The EU AI Act

Obligations along the supply chain - addressees of the EU AI Act

Provider, Art. 3 No. 3

Anyone developing an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge

Distributor, Art. 3 No. 7

Anyone, other than the provider or the importer, that makes an AI system available on the Union market

Importer, Art. 3 No. 6

- located or established in the EU
- special form of distributor
- placing on the market or putting into service of non-European AI systems in the Union

Deployer, Art. 3 No. 4

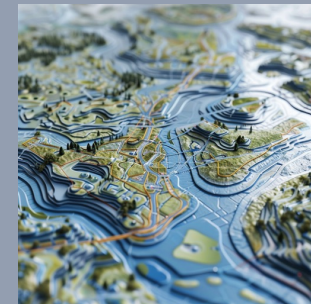
- Professional use of an AI system under your own responsibility
- Companies and organizations using AI systems in the EU

II The EU AI Act

Definition of AI system according to the EU AI Act:

"a machine-based system that is 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"

- AI in remote sensing industry?
- E.g. Software that calculates a forecast of possible flooding scenarios based on training data, topographical maps, satellite data, weather reports and messages on social media



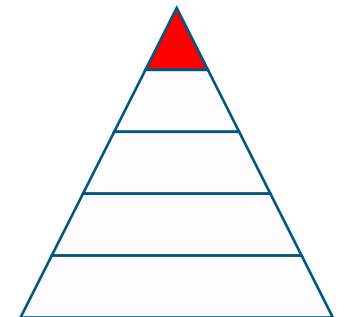
II. The EU AI Act

Prohibited AI Practices

- AI systems or applications that manipulate human behavior to circumvent users' free will
- Systems through which authorities evaluate social behavior (social scoring)
- Biometric remote identification in real time
- Systems for predictive policing
- Categorization based on sensitive characteristics

following a decision in the trilogue:

- Emotion recognition systems no longer prohibited in law enforcement and border protection
- Biometric remote identification in real time and ex-post now permitted in exceptional cases (especially law enforcement)



II. The EU AI Act



High-risk AI

- AI systems with high risk
- divided into two types of categories:

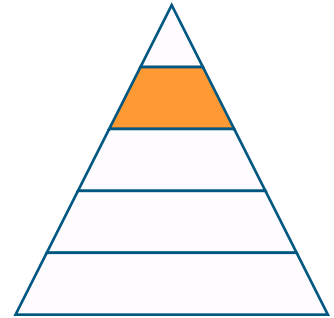
1. Products or safety components of products that are subject to EU product safety legislation and (!) or must undergo a third party conformity assessment before being placed on the market or put into service

2. AI systems listed in Annex II Risk to health, safety and fundamental rights

- Education
- Employment
- Critical infrastructures
- Public services
- Prosecution
- Border controls
- Administration of justice

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(1)
High-risk AI systems pursuant to Article 6(1) are the AI systems listed in any of the following areas:

1. Biometric identification and categorization of natural persons: (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons.
2. Management and operation of critical infrastructures: (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
3. Education and vocational training: (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions. (b) AI systems intended to be used for the purpose of monitoring students in educational and vocational training institutions and for monitoring participants in such courses required for admission to educational institutions.
4. Employment, workers management and access to self-employment: (a) AI systems intended to be used for recruitment or selection of natural persons, enable for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests. (b) AI systems intended to be used for making decisions on promotion and termination of work-related contractual relationships, the task allocation and the monitoring and evaluating performance and behavior of persons in such relationships.
5. Access to and enjoyment of essential private services and public services and benefits: (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, withdraw, revoke, or withdraw such benefits and services. (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems put into service by small-scale providers for their own use. (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid.
6. Law enforcement: (a) AI systems intended to be used by law enforcement authorities for making individual risk assessment of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences. (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person.



II. The EU AI Act

High-risk AI

- AI systems with high risk, divided into two types of categories:

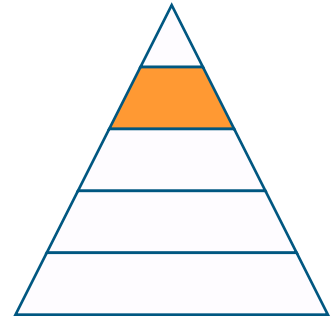
Critical infrastructure: AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity

2. AI systems listed in Annex II Risk to health, safety and fundamental rights

- Education
- Employment
- Critical infrastructures
- Public services
- Prosecution
- Border controls
- Administration of justice

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(1)
High-risk AI systems pursuant to Article 6(1) are the AI systems listed in any of the following areas:

- Biometric identification and categorization of natural persons:
 - (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;
- Management and operation of critical infrastructure:
 - (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity;
- Education and vocational training:
 - (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
 - (b) AI systems intended to be used for the purpose of monitoring students in educational and vocational training institutions and for monitoring participants in such courses required for admission to educational institutions;
- Employment, workers management and access to self-employment:
 - (a) AI systems intended to be used for recruitment or selection of natural persons, enable for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
 - (b) AI systems intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships;
- Access to and enjoyment of essential private services and public services and benefits:
 - (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, withdraw, revoke, or withdraw such benefits and services;
 - (b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems per se services by small-scale providers for their own use;
 - (c) AI systems intended to be used to dispatch, or to establish priority in the dispatching of emergency first response services, including by firefighters and medical aid;
- Law enforcement:
 - (a) AI systems intended to be used by law enforcement authorities for making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending or the risk for potential victims of criminal offences;
 - (b) AI systems intended to be used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person;



II. The EU AI Act

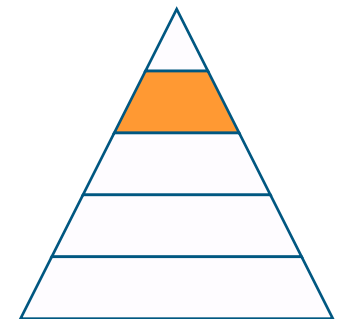
High-risk AI

Requirements for AI systems with high risk, among others:

- Carrying out conformity assessments
- Integration of quality and risk management systems
- Data Quality
- Registration
- **Post-market surveillance by supervisory authorities**

After trilogue: filter system to capture only genuine high-risk AI

- even if the AI system formally falls under the catalog of high-risk AI, it loses its classification if the requirements of the filter system are met
- e.g.: AI only checks or improves human activity or only fulfills narrow procedural tasks

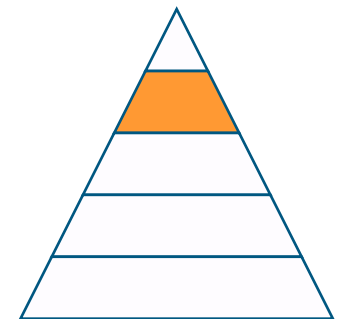


II. The EU AI Act

High-risk AI

Art. 12 EU AI Act – Data and Data Governance


Para. 1: *“High-risk AI systems which make use of techniques involving the training of AI 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 whenever such data sets are used.”*



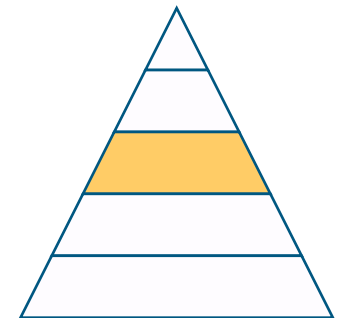
II. The EU AI Act

General Purpose AI Model (GPAI):

- GPAI are the AI technologies on which the generative AI applications are based - in the case of the well-known language model ChatGPT, for example, the GPAI is GPT-4
- Definition should comprehensively cover very large generative AI models
- Welcome exceptions for research, development and prototyping activities



→ Consequence: Obligations for providers of large GPAI (e.g. OpenAI)
→ Consequence: Obligations for deployers of AI on the basis of GPAI



II. The EU AI Act

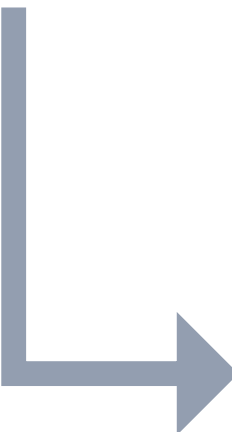
General Purpose AI Model (GPAI):

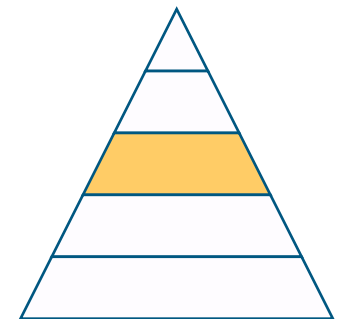
Minimum requirements for all GPAI:

- Technical documentation
- Information for downstream providers and users
- Transparency obligations
- Compliance with copyright laws

Obligations for GPAIs with systemic risks:

- more extensive obligations
- currently only include the largest language models

- 
- GPAIs are not subject to further obligations of the AI Act
→ Obligations will only apply to AI applications

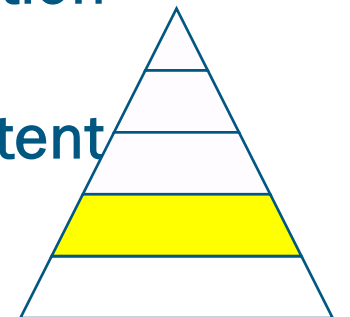


II. The EU AI Act

AI systems that are intended to interact with natural persons

Transparency obligations under Art. 50 EU AI Act

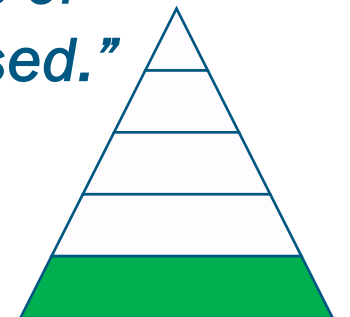
- **Obligation of providers to design AI systems in such a way that it is clear that they are AI when used**
- **Information obligations, including on specific AI-supported functions of the system, human supervision and the person responsible for AI decision-making processes**
- **Users of emotion recognition and biometric categorization systems must provide information about their use**
- **Users who create/manipulate text, audio or visual content with AI must disclose this in some cases**



II. The EU AI Act

Other AI systems (no high-risk AI or GPAI)

- Rather limited „obligations“
- Art. 4 EU AI Act: *“Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.”*



III. Relevance of the EU AI Act for the remote sensing industry

The specific impact of the EU AI Act on companies in the remote sensing industry depends on various factors

- Type of specific AI applications used (in particular, whether high-risk AI or not)
- In most cases, the AI Act will not apply directly to remote sensing companies
- However, they will – especially with data products – contribute to AI systems and therefore, providers will flow down obligations to remote sensing companies

Thus:

- Remote sensing companies must at least familiarize themselves with relevant „indirect“ obligations

IV. Short introduction to the EU Digital Services Act

Objectives

- Adapt the EU legal framework for illegal content on intermediaries (e.g. online platforms)
- Modernization of the e-Commerce Directive adopted in 2000
- Harmonization of EU laws (prior directive had to be transformed into national laws)
- Ban illegal content and disinformation
- Ensure transparent advertising

IV. Short introduction to the EU Digital Services Act

Scope of application

- Intermediary service providers (e.g. online platform providers) offering services to users in the EU, irrespective of whether the intermediary service provider is established in the EU
- Types of intermediaries:
 - Access services, e.g. telephone service providers such as AOL and Deutsche Telekom or internet access services such as T-Online and Vodafone (Art. 3 g) i) EU DSA),
 - Caching services, e.g. CDN providers such as Leaseweb or Fastly (Art. 3 g) ii) EU DSA)
 - Hosting services, e.g. web hosting providers such as Jimdo and online marketplaces such as Etsy or Ebay (Art. 3 g) iii) EU DSA)
 - Online platforms, e.g. social networks such as Facebook and Tik Tok (Art. 3 i) EU DSA) and
 - Online search engines, e.g. Google or DuckDuckGo (Art. 3 j) DSA).

IV. Short introduction to the EU Digital Services Act

Some of the legal obligations

- Obligations depend on the type of intermediary
- Some of the obligations are
 - remove illegal content
 - Only allow targeted advertising in limited circumstances
 - certain reporting obligations
- Further obligations put on “**very large online platforms**” and very “**large online search engines**”
 - Risk assessment
 - Risk mitigation
 - Crisis response mechanism
 - Independent audit
 - Additional online advertising transparency
 - Data access and scrutiny
 - Compliance function
 - Further transparency obligations

IV. Short introduction to the EU Digital Services Act

Why would this be relevant for remote sensing companies?

- List of very large online platforms:
 - Alibaba AliExpress
 - Amazon Store
 - Apple AppStore
 - Booking.com
 - Facebook
 - Google Play
 - Google Maps
 - Google Shopping
 - Instagram
 - LinkedIn
 - Pinterest
 - PornHub
 - [...]

Contact us

BHO Legal

Hohenstaufenring 29-37
50674 Cologne

Phone: + 49 (0) 221 270 956 0

Fax: + 49 (0) 221 270 956 222

cologne@bho-legal.com

Gerhard Deiters

Lawyer | Partner

Phone: + 49 (0) 221 270 956 160

E-mail: gerhard.deiters@bho-legal.com