HERZOG

HERZOG FOX & NEEMAN

The EU Artificial Intelligence Act

Herzog's Guide

March 2024

INTRODUCTION

The European Artificial Intelligence Act (the "AI Act" or the "Act") stands as a pioneering legislative framework, marking the world's **first cohesive and harmonized approach to regulating artificial intelligence**.

The AI Act is aiming to mitigate potential harms and ensure robust oversight. It explicitly **prohibits the use of certain AI systems** deemed unacceptable risks to fundamental rights; imposes **significant regulatory requirements on other AI systems** classified as high-risk; imposes specific regulatory requirements on **general purpose AI systems and models**; and includes additional **transparency regulatory requirements** for some types of AI systems with lower risk. All other AI systems, including those that are not subject to the detailed regulatory requirements, will still be required to take measures to ensure a sufficient level of **AI literacy** in their internal operational and usage level.

Noncompliance with the Act's obligations may result in fines of up to **€15,000,000 or 3% of annual worldwide turnover**, whichever is higher (or smaller fines in case of small-medium enterprises and startups). Fines in case of providing a prohibited AI system could reach as high as €35,000,000 or 7% of annual worldwide turnover.

The AI Act will enter into force 20 days following official publication.

The provisions concerning **prohibited AI systems** will start to apply **6 months following entry into force**. Other significant provisions - concerning **general purpose AI models**, governance, confidentiality, notifying authorities and notified bodies, as well as penalties - will start to apply within **12 months**. The rest of the provisions will start to apply either **24 months** following the entering into force of the Act, or **36 months** in case of some provisions concerning high-risk AI systems subject to EU product safety regulation.

To assist with understanding and navigating between the novel requirements under the AI Act, we are pleased to share **Herzog's Artificial Intelligence Act Guide**, providing explanation about its scope, key practical takeaways and insights.

OVERVIEW OF THE ACT

Key Definitions

- **AI system -** 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. This definition is **not intended to cover simpler traditional software systems or programming approaches**, which are based on the rules defined solely by natural persons to automatically execute operations. AI systems can be used on a **stand-alone basis** or as a **component of a product**, irrespective of whether the system is physically integrated into the product (embedded) or serve the functionality of the product without being integrated therein (non-embedded).

- **General purpose AI model ("GPAI model") -** an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.

- **General purpose AI system ("GPAI systems") -** an AI system which is based on a GPAI model, that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

ROLES IN THE AI SYSTEM SUPPLY CHAIN

Provider

Develops or supplies the AI system or GPAI model under its name or trademark.

Deployer (user)

Uses the AI system in the course of a non-personal professional activity.

Importer

Established in the EU. Supplies an AI system in the EU for a non-EU Provider.

Distributor

Person or entity, which is not a provider or importer, that makes an AI system available in the EU without affecting its properties.

SCOPE OF APPLICATION

The Act applies to:	Exemptions:
✓ Providers **supplying** AI systems and GPAI models **in the EU** (whether the provider is established or located in the EU or not);	✗ Areas outside the scope of EU law;
✓ Deployers of AI systems **established or located in the EU**;	✗ **Exclusive military, defense** or national security purposes;
✓ Providers and deployers outside the EU, where the output of the AI system **is used in the EU**;	✗ Systems developed and used for the sole purpose of **scientific R&D**;
✓ Importers, distributors and authorized representatives.	✗ **Research, testing** and **development** activities of an AI system of models, before supplying them, in **testing environment** only;
✓ Product manufacturers **supplying in the EU** an AI systems, together with their product, **under their own name or trademark**;	✗ **Non-EU public authorities** and international organizations using AI systems in the framework of international cooperation or agreements for **law enforcement and judicial cooperation** with the EU, subject to the provision of adequate safeguards;
✓ Affected persons located in the EU.	✗ **Purely personal non-professional** uses by individuals;
	✗ AI systems under **free and open-source licenses,** which do not fall under one of the risk categories under the Act (prohibited, high-risk, and systems subject to transparency obligations).

PROHIBITED AI PRACTICES

The following AI practices are prohibited under the AI Act:

- AI systems using **manipulative** and **deceptive** techniques or **exploiting people's vulnerabilities** due to age, disability or social or economic situation to distort their behavior in a manner that causes or reasonably likely to cause them significant harm.

- Risk assessment **for predicting the risk of a person to commit a criminal offence**, based **solely** on their personality traits and characteristics. This shall not apply to systems used to support the human assessment of a person's involvement in a crime, which is already based on facts linking them to that crime.

- **Biometric categorization** systems used to deduce or infer peoples' race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. Not including labeling or filtering lawfully acquired biometric datasets, in the area of law enforcement.

- **Social scoring** systems leading to detrimental or unfavorable treatment in social contexts **unrelated to the contexts** in which the data was originally generated or collected; or that is **unjustified** or **disproportionate** to their social behavior or its gravity.

- Real-time **remote biometric identification in publicly accessible** spaces for law enforcement purposes, unless the use is strictly necessary for certain objectives such as: searching for a crime victim, prevention of substantial and imminent threat to life or physical safety, locating suspects of serious crimes.

- **Emotion inference** in areas of workplace and education institutions, except for systems used for medical or safety reasons.

- Untargeted **scraping for facial recognition** from the internet or CCTV footage.

HIGH-RISK AI SYSTEMS

What is defined as high risk AI systems?

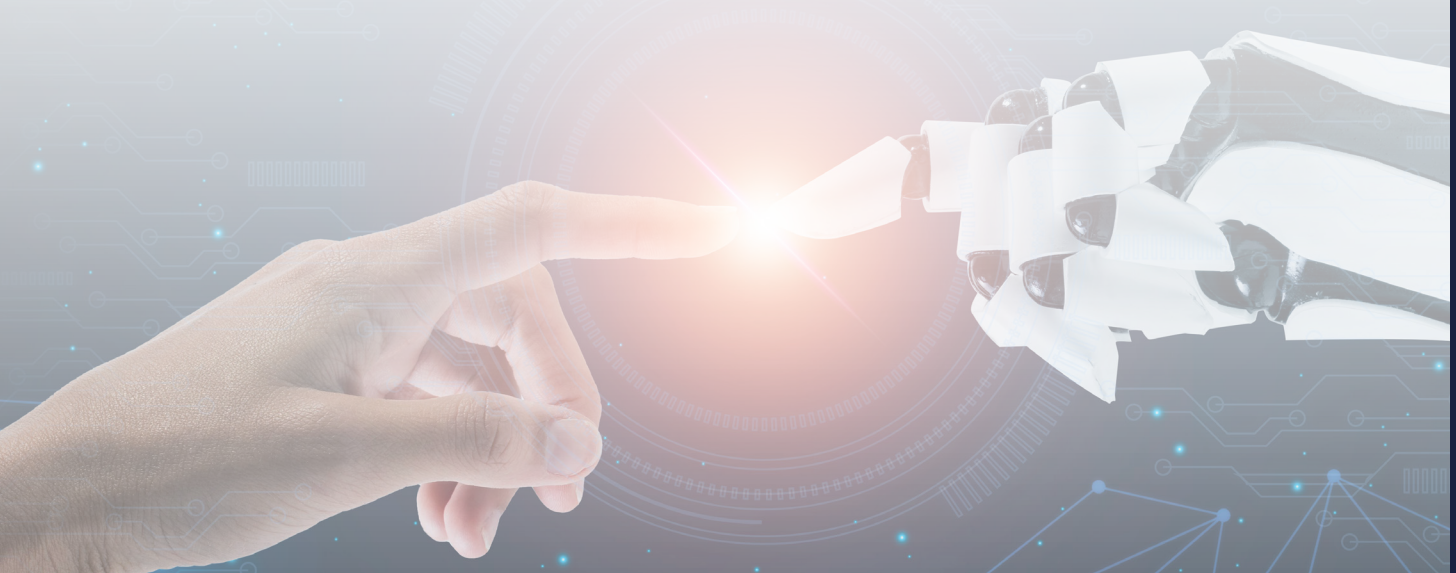
Main part of the AI Act imposes requirements on what is defined as **high risk AI systems.** According to the AI Act, high risk AI systems are the ones that fall under one of the following categories:

1. Products that are subject to EU product safety legislation

AI systems which are **products** - or **safety components of products** - subject to EU product safety legislation, and are required to undergo a **third-party conformity assessment** under such legislation before being supplied in the EU.

This includes products in the areas such as:

- Machinery
- Toys
- Recreational boats and watercraft
- Lifts
- Personal protective equipment
- Radio equipment
- Fuels
- Medical devices



2. AI systems in critical areas

In addition to the first category, the AI Act defines as high risk, AI systems that are being **used in defined critical areas**, in a way that may impose **significant risk of harm** to the health, safety or fundamental rights.

The 8 critical areas listed in the relevant annex of the Act are:

- **Biometric identification** and categorization and emotion recognition
- **Critical infrastructure**
- **Education** and vocational training
- **Employment**, workers management and access to self-employment
- Access to and enjoyment of essential private services and essential public services and benefits (including **credit scoring**, evaluating and classification of **emergency calls**, and risk assessment and pricing of **life and health insurance**)
- **Law enforcement**
- **Migration**, asylum and border control management
- Administration of **justice** and **democratic processes**

An AI system that is used in the abovementioned critical areas, but is **not considered as posing a significant risk of harm** to the health, safety or fundamental rights, including by not materially influencing the outcome of decision making (and will **therefore not be considered high risk**), is a system that is intended to do one or more of the following:

- perform a **narrow procedural task**;
- improve the result of a **previously completed human activity**;
- detect decision-making **patterns** or **deviations** from prior decision-making patterns, and is **not meant to replace or influence** the previously completed human assessment, without proper **human review**;
- perform a **preparatory task** to an assessment relevant for the purpose of the use cases listed in Annex III of the Act.

Relying on the above derogations is subject to the performance of appropriate and documented **assessments before placing** the AI system on the market, as well as registration requirements.

Despite the above, an AI system shall always be considered high-risk if it performs **profiling of natural persons**.

REGULATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

System requirements

Risk management system

A risk management system must be **established**, **documented**, and **maintained throughout the AI system's lifecycle**.

- Such system involves identifying, analyzing, and evaluating **risks** to health, safety, or fundamental rights, including risks from intended use and reasonably foreseeable misuse, as well as post-market monitoring data.
- It requires adopting **targeted measures** to mitigate identified risks, ensuring that any residual risk is acceptable.
- The process includes the **design** and **development** of the AI system, implementation of **mitigation measures**, and **provision of information** and training to deployers.
- Risk management also involves **testing** the AI system against defined metrics to ensure compliance and consistent performance for its intended purpose.

Data and data governance

High-risk AI systems which make use of techniques involving the training of models with data must be developed with data on the basis of **training**, **validation** and **testing datasets** that meet specific quality criteria.

- These datasets must undergo proper **data governance** and **management** practices tailored to the AI system's purpose, addressing aspects such as **design choices**, **data collection, processing operations**, **bias mitigation**, and data **gap identification**.
- Data must be **relevant**, **representative**, **error-free**, and **complete**, considering the specific contexts and characteristics of the intended application area.

Technical documentation

Technical documentation must be prepared **before high-risk AI systems are placed on the market** or put into service and shall be kept **up-to-date**.

- It should provide necessary **information for compliance assessment** and contain certain information (outlined in the relevant annex of the Act) about the AI system, its process of development, its monitoring, functioning and control and more.
- **Small-medium enterprises** and **start-ups** may provide the technical documentation in a **simplified manner**.

Record-keeping

Automatic **logging capabilities** must be included to trace the AI system's functioning throughout its lifecycle, including identifying potential risks, facilitating **post-market monitoring**, and **overseeing the operation** of high-risk AI systems.

- Certain high-risk AI systems shall include additional specific logging capabilities.

Transparency and information to deployers

High-risk AI systems must be designed for **operational transparency** to enable deployers to interpret the system's output and use it appropriately.

- These systems must be accompanied with **clear instructions** detailing the system's characteristics, capabilities and imitations, including the system's intended use, level of accuracy, robustness and cybersecurity, potential risks, and conditions affecting performance.
- Instructions should also cover **human oversight measures**, necessary **computational resources**, **system maintenance**, and **logging guidelines**.

Human oversight

High-risk AI systems must include **human oversight mechanisms** to prevent or minimize risks to health, safety and fundamental rights.

- Measures for oversight should be **built into the system** or be **implementable** by the user.
- In order to ensure effective human control, the systems should be designed to enable human overseers to properly **understand** the system, **monitor** operations, recognize and mitigate **automation bias**, **interpret** outputs accurately, and maintain the option to **disregard**, **override** or **reverse** the output or halt the system as needed.

Accuracy, robustness, and cybersecurity

High-risk AI systems must be designed and developed for appropriate level or accuracy, robustness, and cybersecurity, **maintaining these standards throughout their lifecycle**.

- Systems should be resilient to **errors**, **faults**, and **environmental inconsistencies**, including interactions with humans or other systems, employing measures like technical redundancy solutions for robustness, which may include backup or fail-safe plans.
- For **AI systems that continue to learn** after deployment, measures must appropriately **mitigate biased feedback loops**.
- The system must be protected against **unauthorized alterations**, with defenses against **data and model poisoning**, adversarial examples, and other vulnerabilities, ensuring the **system's integrity** against manipulation or attacks.

Post-deployment requirements

Post-market monitoring

In order to allow the provider to **evaluate the continuous compliance** of AI systems with the requirements of the Act, providers of high-risk AI systems are required to **establish** and **document** a post-market monitoring system that will actively and systematically **collect**, **document** and **analyze** relevant data on the performance of high-risk AI systems throughout their lifetime.

- The post-market monitoring system will be based on a post-market **monitoring plan**, which will be part of the system's technical documentation.

Reporting of serious incidents

Providers of high-risk AI Systems **which are placed on the EU market**, are required to report a serious incident to the market surveillance authorities of the Member States where that incident occurred.

- The notification should be made **immediately** after the provider has established a link between the AI system and the serious incident or the reasonable likelihood of such a link, and **no later than 15 days** after becoming aware of the incident (or 10 days in the event of death of a person).
- Following the reporting, the provider shall **co-operate** with the competent authorities and perform the **necessary investigations**, including a risk assessment of the incident and corrective action.

Demonstrating compliance and conformity requirements

Conformity assessment

High-risk AI systems must undergo one of two types of **conformity assessment procedures**, as per the Act's applicable requirements to the AI system's type:

1. **Self-assessment** based on internal controls according to the procedure detailed in the Act.

2. **Third-party assessment** based on assessment of the quality management system and the technical documentation, with the involvement of a **notified body** according to the procedure in the Act. The notified body will issue a **conformity certificate**.

High-risk AI systems subject to EU **product safety legislation** - shall undergo the relevant conformity assessment **as required under the applicable safety legislation**, and the requirements under the AI Act shall be part of that assessment.

High-risk AI systems used in the Act's defined **critical areas:**

• High-risk AI systems used in all critical areas listed in the Act (page 8 above), *besides* biometric identification and categorization and emotion recognition - shall follow the **self-assessment** procedure.

• High-risk AI systems used in **biometric identification and categorization and emotion recognition**, must undergo a **third-party assessment**, unless the provider has relied on recognized standardization to be published by the European Commission (harmonized standards or common specifications).

All high-risk AI systems must undergo a **new conformity assessment** procedure whenever they are **substantially modified**.

EU declaration of conformity

Providers of high-risk AI systems shall draw up and sign a **declaration of conformity** asserting compliance with the requirements of the AI Act. The declaration should contain all the information specified in the Act, be **kept for 10 years** and presented to the competent authorities upon request.

CE marking of conformity

High-risk AI systems should be affixed with **CE marking indicating compliance** with the requirements of the AI Act and other legislation (if relevant). The CE marking must be affixed in a visible, legible, and indelible manner or digitally accessible for digital systems.

Registration

Providers (or, where applicable, the authorized representative) of high-risk AI systems used in the defined critical areas, shall register **themselves and their system** in a **designated EU database**. This obligation shall also apply to deployers who are public authorities, agencies or bodies or persons acting on their behalf.

High-risk AI systems used in **critical infrastructure** shall be registered at national level.

ROLE-SPECIFIC REGULATORY REQUIREMENTS FOR HIGH-RISK AI SYSTEMS

In addition to the requirements that apply to the high-risk AI systems itself, the AI Act imposes role-specific obligations for the operators of such AI systems.

Providers

- Ensure compliance with the **AI system requirements**.
- Establish **quality management system** including written policies, procedures and instructions.
- **Record and logs keeping** obligations.
- Ensure the AI system undergoes the relevant **conformity assessment**.
- Draw up an **EU declaration of conformity**.
- Affix **CE marking** to the AI system.
- EU database **registration**.
- Appoint **authorized EU representatives** (for non-EU providers).
- Indicate name, trademark and address on the AI system.
- Ensure compliance with **accesibility requierments**.
- **Inform** the competent authorities in case of **identified risks**.
- **Cooperate** with compenent authorities.

Deployers (users)

- Use the system according to **instructions**.
- Assign **human oversight** to a person with necessary competence, training and authority.
- Ensure **input data** is relevant and sufficiently representative, in view of the system's intended purpose.
- **Inform** in case of identified risk, incident or malfunction.
- Keep **logs** that are under their control (at least 6 months).

- **AI at the workplace** - deployers who are employers shall inform workers representative and affected workers that they will be subject to the system.
- **EU database registration** - only applicable to public authorities, agencies or bodies or persons acting on their behalf.
- Perform a **fundamental rights impact assessment** – only applicable to deployers governed by public law, private actors providing public services, and deployers using high risk AI systems intended to establish credit score or to be used for risk assessment and pricing for life and health insurance.
- **Cooperate** with competent authorities.

Importers

- **Ensure the AI system complies with the AI Act.** This includes verifying that the provider has conducted a conformity assessment, drawn up the technical documentation and appointed an authorized representative, and that the AI system bears the requiered CE marking and is accompnied by the EU decleration of conformity.
- **Record-keeping** obligations.
- **Inform** in case of **identified risk**.
- Do not jeopardize compliance while the AI system is under your control.
- Indicate name, trademark and address on the AI system.
- **Cooperate** with competent authorities.

Distributors

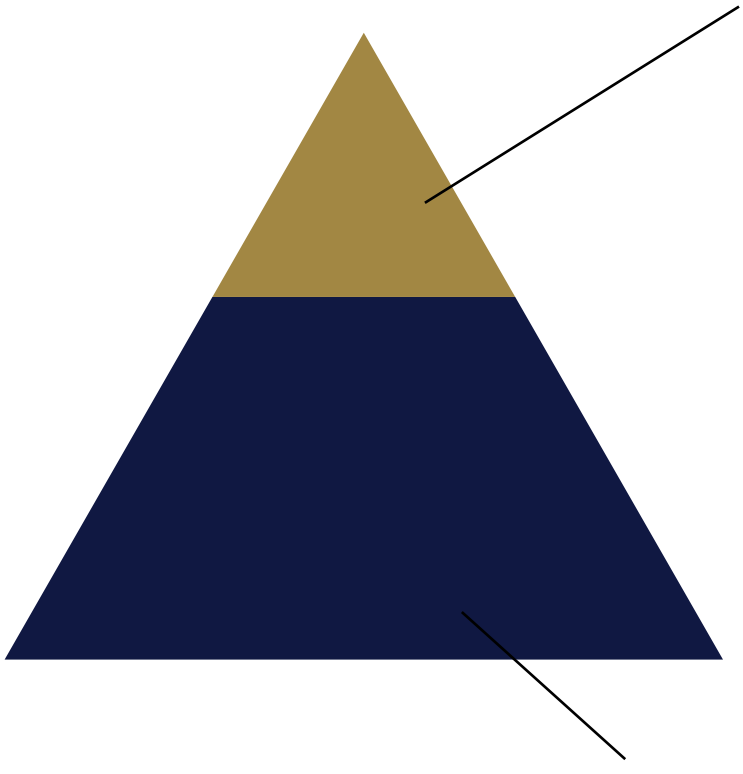
- Verify the systems bears **required CE marking** and in accompanied by an **EU declaration of conformity** and **instructions of use**.
- Verify that the AI System carries the **name**, **trademark and address** of the provider and/or importer.
- **Inform** in case of identified risk.
- Do not jeopardize compliance while the AI system is under your control.
- **Inform** in case of identified risk.
- **Cooperate** with competent authorities.

GENERAL PURPOSE AI MODELS

GPAI models risk classification

The **Act classifies GPAI models** into two groups:

1. GPAI models **without systemic risk**; and
2. GPAI models **with systemic risk:**



A GPAI model **without systematic risk.**

A GPAI model **with systemic risk** is a model that meets any of the following criteria:

(a) it has **high impact capabilities** evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks (providers of such models should provide a notification to the EU Commission within 2 week);

(b) it is subject to a **decision of the EU Commission**, that the model has capabilities or impact equivalent to those of point (a).

When the cumulative amount of compute used for the model's training measured in floating point operations (FLOPs) is greater than 10^25 – the model will be presumed to have ' high impact capabilities'.

The provider of a model that should originally be clasified as having high impact capabilities may present, in its notification to the Commission, **arguments** to demonstrate that the model, due to its specific characteristics, **does not present a "systematic risk"** and should therefore be classified as a "regular" GPAI model.

Regulatory obligations for GPAI models

The following table summarizes the obligations for GPAI models under the AI Act:

Obligation	Regular GPAI	Systemic Risk GPAI
Technical documentation & information sharing		
Technical documentation, including training and testing processes and evaluation results	✓*	✓
Sharing documentation and information with providers integrating the model	✓*	✓
Model evaluation, including adversarial testing, with a view to identify and mitigate systemic risk	✗	✓
Assessment and mitigation of possible systemic risks at EU level	✗	✓
Reporting and cybersecurity		
Documenting and reporting serious incidents and corrective measures to the AI Office and national authorities	✗	✓
Ensuring adequate cybersecurity protection of the model and its physical infrastructure	✗	✓
Copyright and training content summary		
Implementing a policy to respect EU copyright law	✓	✓
Publishing a detailed summary of training content	✓	✓
Cooperation and compliance		
Cooperation with the Commission and national authorities	✓	✓
EU authorized representative (for non EU-providers)	✓*	✓

* Not applicable to models accessible under a free and open license, where comprehensive technical information about the model is publicly available.

TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS AND GPAI MODELS

While high-risk AI systems and GPAI models are subject to substantial regulatory requirements, as detailed in the previous chapters, there are AI systems and models that are **subject to specific transparency obligations**. If such AI systems are also classified as high-risk, the following obligations apply **in addition** to the requirements for high-risk AI systems. If the systems are not classified as high-risk, only the following limited obligations apply.

The information provided as per these transparency obligations shall be:

- Provided in a **clear** and **distinguishable** manner at the latest at the time of the **first interaction or exposure**, and
- respect the applicable **accessibility requirements**.

AI systems intended to interact with natural persons

- The person must be **informed** that they are interacting with an AI system in a **timely**, **clear and intelligible** manner (unless this is obvious from the point-of-view of the person using the system, considering the circumstances and the context of use).
- Exemptions: AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences, subject to appropriate safeguards, unless those systems are available for the public to report a criminal offence.

AI and GPAI systems generating synthetic audio, imgae, video or text content

- Outputs must be **marked** in a machine-readable format and **detectable** as artificially generated or manipulated.
- The implemented technical solutions should be effective, interoperable, robust, and reliable to the extent technically feasible, considering the content's specificities, implementation costs, and state-of-the-art standards.
- Exemptions: AI systems performing an assistive function for standard editing or that do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorized by law to detect, prevent, investigate and prosecute criminal offences.

Emotion recognition system or a biometric categorization systems

- Deployers shall **inform** the persons exposed to the system of the operation of the system and process the personal data collected in accordance with the **GDPR** and other laws pertaining to personal data.
- Exemptions: AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences, subject to appropriate safeguards.

"Deep fake" AI systems

- "Deep fake" means AI generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful.
- Deployers shall **disclose** that the content has been **artificially generated or manipulated**.
- Where the content forms part of an **evidently artistic**, **creative**, **satirical**, **fictional or analogous work** – the transparency obligations should not hamper the display or enjoyment of the work.
- Exemptions: AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences.

AI systems that generate or manipulate text for informing the public on matters of public interest

- Deployers shall **disclose** that the text has been **artificially generated or manipulated**.
- Exemptions:
  - AI systems authorized by law to detect, prevent, investigate and prosecute criminal offences.
  - AI-generated content that has undergone a process of human review or editorial control, where the editor holds responsibility for the publication of the content.

HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique set of vital, **interdisciplinary** and **global** regulatory advisory skills, and are uniquely positioned to advise a range of clients, including leading multinational technology companies as well as start-ups and disruptive technologies vendors, on applicable regulatory and compliance considerations in numerous technological areas.

We understand that the **regulatory exposure** and scope of required **attention** of almost any company operating in the **digital and technological sphere** are much wider than one specific jurisdiction or legal discipline. As our clients are often on the forefront of this ever-evolving landscape, we further understand the impact of industry trends and compliance demands on our clients' businesses. Therefore, our team possesses in-depth knowledge of the increasing volume of regulations, enforcement actions, legislative and industry trends in a **myriad of jurisdictions**, **digital platforms** and leading **self-regulatory guidelines**. This enables our team to offer **practical**, **holistic** and **comprehensive** solutions for complex situations often presented by innovative technologies and disruptive business solutions, providing "hands-on" support to our clients on the strategic, corporate and operational aspects of their business, with the aim of mitigating our clients' legal and business risks.

Artificial Intelligence technologies are reshaping familiar industries and bring them to new exciting frontiers which raise novel fascinating legal and regulatory challenges. AI has recently come to the forefront of the regulatory and legislative trends globally, and are now subject to the increased of focus of legislators and regulators in a wide array of jurisdictions. Alongside the emerging **bespoke regulatory frameworks**, AI systems are also subject to various **existing general and sector specific legal and regulatory regimes**, as well as self-regulatory guidelines which lie down at the intersection of law and technology.

Our unique AI law practice is led by top legal experts and professionals with deep legal, regulatory as well as technical understanding and hands-on background in AI, machine learning, deep learning and neural networks technologies. This enables us to offer tailor made and practical solutions for often complex situations, and to assist in the **development**, **implementation**, **management and use** of adequate and **compliant AI technologies**, thereby mitigating legal and business risks.

HERZOG
HERZOG FOX & NEEMAN

The EU Artificial Intelligence Act

Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il

Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il

Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il

Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il

Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il

Dima Zalyalyeyev | Associate
Technology Regulation
zalyalyeyevd@herzoglaw.co.il

Or Noy | Associate
Technology Regulation
noyo@herzoglaw.co.il

On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il

Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il

Oded Kramer | Associate
Technology Regulation
kramero@herzoglaw.co.il

Michal Kra | Associate
Technology Regulation
kram@herzoglaw.co.il

Mai Arlowski | Associate
Technology Regulation
arlowskim@herzoglaw.co.il

Yonatan Glatt | Associate
Technology Regulation
glatty@herzoglaw.co.il

Liron Adar | Intern
Technology Regulation
adarl@herzoglaw.co.il

Kobi Plotkin | Intern
Technology Regulation
plotkiny@herzoglaw.co.il

Eden Lapid | Intern
Technology Regulation
lapide@herzoglaw.co.il

Neriya Rettig | Intern
Technology Regulation
rettign@herzoglaw.co.il

Yuval Glezer | Intern
Technology Regulation
glezery@herzoglaw.co.il