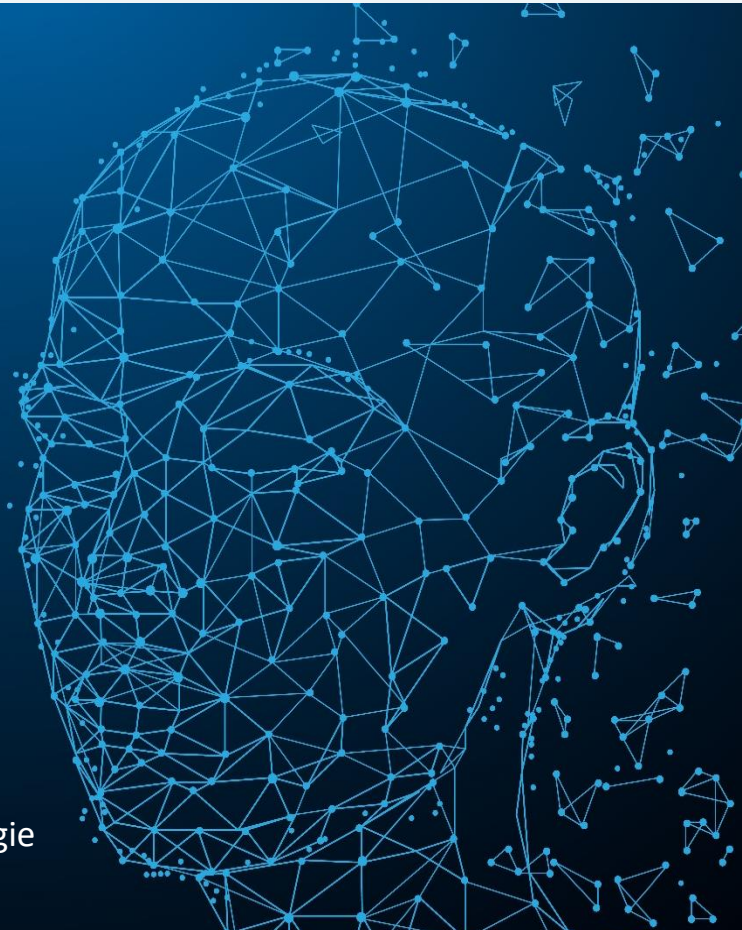
Bundesministerium
Finanzen

bmf.gv.at

Die KI-VO im Überblick

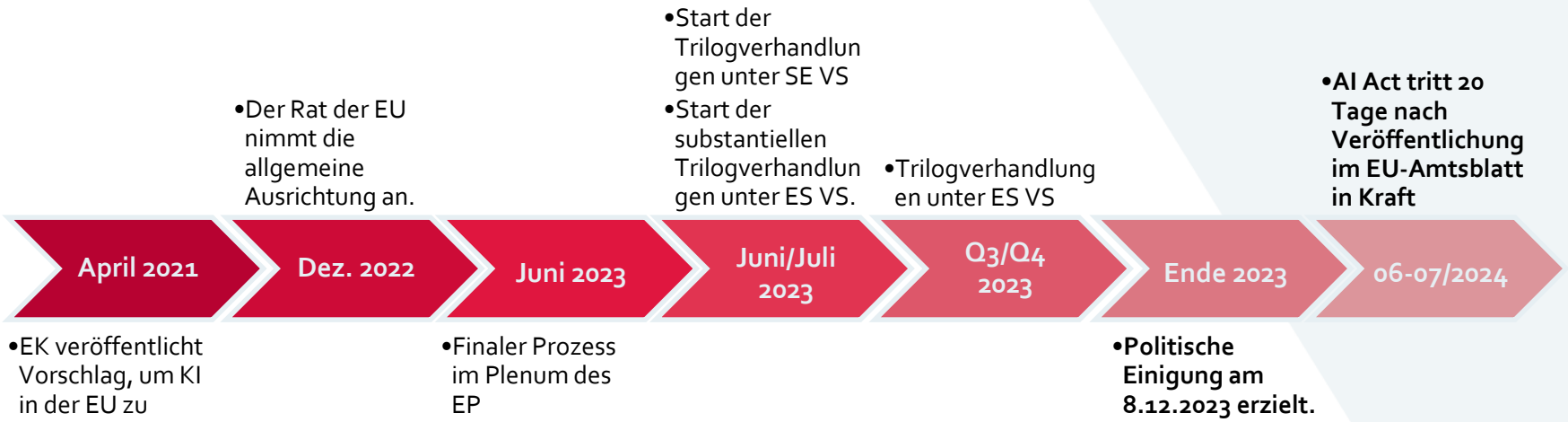


Mag. Julia Fuith, BA LL.M.
BMF - Internationale Beziehungen und Legistik, E-Government-Strategie
25. April 2024

Gliederung

- Timeline der Verhandlungen
- Kurzer inhaltlicher Überblick (und Systematik der Verordnung)
- Entstehungsprozess ausgewählter wichtiger Bestimmungen
- Governance / nationale Umsetzung

Timeline


April 2021
•EK veröffentlicht Vorschlag, um KI in der EU zu regulieren
Dez. 2022
•Der Rat der EU nimmt die allgemeine Ausrichtung an.
Juni 2023
•Finaler Prozess im Plenum des EP
•13.6 Diskussion im Plenum und Abstimmung
Juni/Juli 2023
•Start der Trilogverhandlungen unter SE VS
•Start der substantiellen Trilogverhandlungen unter ES VS.
Q3/Q4 2023
•Trilogverhandlungen unter ES VS
Ende 2023
•Politische Einigung am 8.12.2023 erzielt.
06-07/2024
•AI Act tritt 20 Tage nach Veröffentlichung im EU-Amtsblatt in Kraft

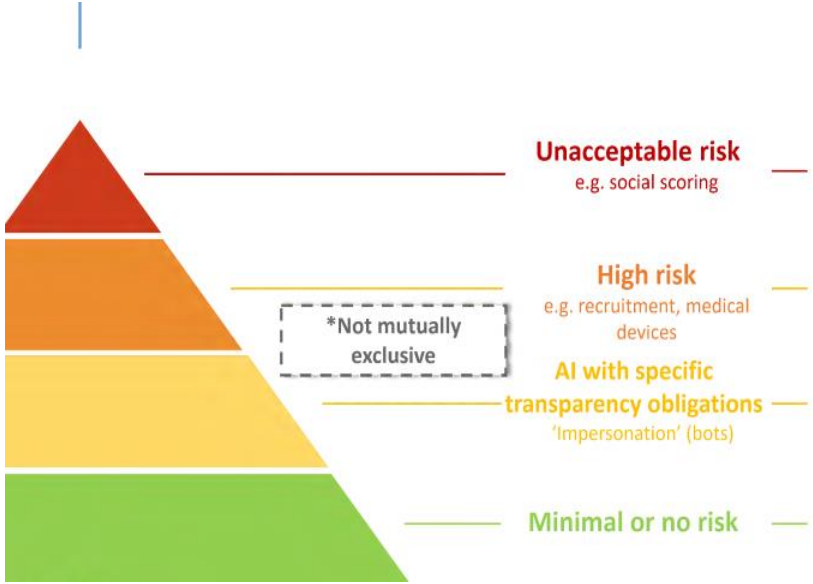
Inhalt des KI-VO-Vorschlags im Überblick

- **Harmonisierung der Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen in der EU**
- **Verbot bestimmter Praktiken** im KI Bereich
- **Anforderungen** an Hochrisiko-KI-Systeme
- **Verpflichtungen** für Betreiber und Nutzer
- harmonisierte **Transparenzvorschriften** für bestimmte KI-Systeme
- Vorschriften für **Marktbeobachtung**, **Marktüberwachung und Governance**
- Vorschriften zur **Innovationsförderung**

Ausnahmen vom Anwendungsbereich

- KI-Systeme im Bereich **nationale Sicherheit, Verteidigung und für militärische Zwecke**
- KI-Systeme und deren Ergebnisse, die ausschließlich zu **Forschungs- und Entwicklungszwecken** eingesetzt werden
- KI-Systeme, die von **natürlichen Personen im Rahmen einer ausschließlich persönlichen und nicht beruflichen Tätigkeit** verwendet werden
- KI-Systeme, die unter **freien und quellenoffenen Lizenzen** bereitgestellt werden (Ausnahme: Inverkehrbringen/Inbetriebnahme als HR-KI-System oder KI-System, das unter Art 5 oder Art 50 fällt)

Risikobasierter Ansatz der Regulierung

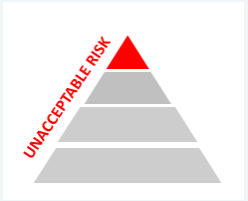


Unannehmbares Risiko: Verbot, da mit Grundrechten nicht vereinbar (z.B. *social scoring*).

Hohes Risiko: hohes Störungsrisiko für menschliches Leben (z.B. Filter bei Bewerbungsprozessen);

Geringes Risiko (z.B. *Chatbots*): Zulässig, jedoch Normierung besonderer Transparenzverpflichtungen;

Minimales Risiko (Großteil der Anwendungen; z.B. Spam-Filter): freie Anwendung auf Basis der bestehenden rechtlichen Verpflichtungen ohne zusätzliche Auflagen



Verbotene Praktiken (Art 5)

- KI-Systeme, die **Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einsetzen** und damit dazu führen, dass Verhalten wesentlich zu beeinflussen oder körperliche/psychische Schäden zufügen.
- KI-Systeme, die **Schwächen oder besondere Umstände** einer Person aufgrund ihres **Alters, einer Behinderung** oder einer bestimmten **sozialen oder wirtschaften** Situation **ausnutzen**.
- KI-Systeme zur **Bewertung oder Klassifizierung natürlicher Personen** über einen bestimmten Zeitraum hinweg auf der Grundlage ihres **Sozialverhaltens oder bekannter oder vorhergesagter persönlicher oder persönlichkeitsbezogener Merkmale** (***social scoring***).
- KI-Systeme zur **Bewertung des Risikos**, dass eine **natürliche Person eine Straftat** begeht (ausschließlich auf der Grundlage ihres Profils oder der Bewertung ihrer Persönlichkeitsmerkmale und Eigenschaften) (***Predictive policing***)
- KI-Systeme zur **Erstellung von Gesichtserkennungsdatenbanken** durch **ungezieltes Auslesen von Gesichtsbildern** aus dem Internet oder Videoüberwachungsanlagen
- KI-Systeme zur **Emotionserkennung** am Arbeitsplatz und im Bildungsbereich
- KI-Systeme zur **biometrischen Kategorisierung** basierend auf sensiblen Merkmalen (z.B. Rasse, politische Meinung, religiöser Glauben, sexuelle Orientierung usw)
- **Biometrische Echtzeit-Fernidentifizierungssysteme** in **öffentlich zugänglichen** Räumen durch **Strafverfolgungsbehörden** zu **Strafverfolgungszwecken** (mit Ausnahmen)

KI-Systeme mit hohem Risiko: zwei Gruppen

1. KI-Systeme, die **Sicherheitskomponenten** von **bereits regulierten Produkten** gemäß sind, und bereits einem Konformitätsbewertungsverfahren durch Dritte unterzogen werden (z.B. medizinische Geräte, Maschinen) => **ANNEX II**

2. Bestimmte **eigenständige KI-Systeme** gemäß **ANNEX III** in den folgenden Bereichen:

- Biometrik
- Kritische Infrastrukturen
- Allgemeine und berufliche Bildung
- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
- Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

Klassifizierung von HR-KI-Systemen

- Art 6 legt in seinem Abs 3 fest, wann KI-Systeme nicht als hochriskant eingestuft werden sollen:
  - **Kein erhebliches Risiko für die Gesundheit, die Sicherheit oder die Grundrechte natürlicher Personen**, auch nicht durch eine wesentliche Beeinflussung des Ergebnisses der Entscheidungsfindung
  - Eine oder mehrere dieser Kriterien müssen erfüllt sein:
    - KI-System für die Erfüllung einer engen begrenzten verfahrenstechnischen Aufgabe,
    - KI-System zur Verbesserung des Ergebnisses einer zuvor durchgeführten menschlichen Tätigkeit,
    - KI-System zur Erkennung von Entscheidungsmustern oder Abweichungen von früheren Entscheidungsmustern zu erkennen,
    - KI-System für die Durchführung einer vorbereitenden Aufgabe für eine in Anhang III aufgeführten Anwendungsfälle relevant ist

Verpflichtungen für Anbieter von KI-Systemen mit hohem Risiko

Neue Vorschriften für Anbieter von KI-Systemen mit hohem Risiko

Schritt 1

Ein KI-System mit hohem Risiko wird entwickelt.

Schritt 2

Es muss der Konformitätsbewertung unterzogen werden und den KI-Anforderungen genügen. Bei einigen Systemen wird eine notifizierte Stelle einbezogen.

Schritt 3

Registrierung eigenständiger KI-Systeme in einer EU-Datenbank

Schritt 4

Eine Konformitätserklärung ist notwendig. Das KI-System muss die CE-Kennzeichnung tragen. Das System kann in Verkehr gebracht werden.

Bei wesentlichen Änderungen im Lebenszyklus des KI-Systems greift Schritt 2.

Grundrechtliche Folgenabschätzung

- **Art 27**
  - Einführung dieser Verpflichtung erst im Rahmen der politischen Einigung im Trilog
  - Gilt für folgende Betreiber
    - Einrichtungen öffentlichen Rechts + private Akteure, die öffentliche Dienstleistungen erbringen
    - Bank- und Versicherungsdienstleister, die KI-Systeme einsetzen, die in Anhang III Nummer 5 lit b und lit d als Hochrisikosysteme aufgeführt sind.
  - Durchführung (vor Inbetriebnahme des KI-Systems) nur für Aspekte, die nicht durch andere rechtliche Verpflichtungen abgedeckt sind, wie z. B. die Datenschutz-Folgenabschätzung gemäß der DSGVO
  - Mitteilung an Marktüberwachungsbehörde nach Durchführung der Folgenabschätzung mittels Fragebogen (wird durch Amt für KI zur Verfügung gestellt)

Maßnahmen zur Innovationsförderung

- **KI-Reallabore**
  - Entwicklung, Erprobung und Validierung innovativer KI-Systeme
  - für einen begrenzten Zeitraum
  - vor ihrem Inverkehrbringen oder ihrer Inbetriebnahme
  - Regulatorische Aufsicht und Anleitung durch zuständige Behörde
- **Möglichkeit des Testens unter realen Bedingungen außerhalb von KI-Reallaboren**
- **Maßnahmen für Kleinanbieter und Kleinnutzer**
  - vorrangiger Zugang zu KI-Reallaboren
  - Gebühren für Konformitätsbewertung proportional zur Unternehmens- und Marktgröße

Entstehungsprozess einiger ausgewählter wichtiger Bestimmungen

- Art 2 (insb. Ausnahmen vom Anwendungsbereich)
- Art 3 Z 1: Definition eines KI-Systems
- Art 5: Verbotene Praktiken (insb. biometrische Fernidentifizierung in Echtzeit an öffentlichen Plätzen zu Strafverfolgungszwecken)
- Art 6: Klassifizierung von HR-KI-Systemen; Anhang III: HR-KI-Anwendungen
- Bestimmungen betr. KI-Systemen mit allgemeinem Verwendungszweck („GPAI“) / „Basismodelle“

Hinweis: Nummerierung der Textversion nach politischer Einigung entspricht dem bereinigten finalen Text nach der sprachjuristischen Überarbeitung (Bezugnahme auf EN Sprachfassung, da die DE Sprachfassung zum Zeitpunkt der Erstellung der Präsentation formell noch nicht verabschiedet wurde).

Art 2 – Ausnahmen vom Anwendungsbereich (1/5)

Nationale Sicherheit / militärische Zwecke:

- **EK-Vorschlag:**

Art 2 (3): This Regulation shall not apply to AI systems developed or used exclusively for military purposes.

- **Allgemeine Ausrichtung:**

Art 2 (3):

This Regulation shall not apply to AI systems if and insofar placed on the market, put into service, or used with or without modification of such systems for the purpose of activities which fall outside the scope of Union law, and in any event activities concerning military, defence or national security, regardless of the type of entity carrying out those activities.

In addition, this Regulation shall not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union for the purpose of activities which fall outside the scope of Union law, and in any event activities concerning military, defence or national security, regardless of the type of entity carrying out those activities.

Art 2 – Ausnahmen vom Anwendungsbereich (2/5)

Nationale Sicherheit / militärische Zwecke:

- **Text nach politischer Einigung:**

Art 2 (3):

This Regulation does not apply to areas outside the scope of EU law and in any event shall not affect the competences of the Member States concerning national security, regardless of the type of entity entrusted by the Member States with carrying out tasks in relation to those competences.

This Regulation does not apply to AI systems if and insofar placed on the market, put into service, or used with or without modification of such systems exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

Art 2 – Ausnahmen vom Anwendungsbereich (3/5)

Wissenschaftliche Forschung und Entwicklung:

- **EK-Vorschlag:**

Keine entsprechende Regelung.

- **Allgemeine Ausrichtung:**

Art 2 (6):

This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

Art 2 (7):

This Regulation does not apply to any research and development activity regarding AI systems.

Art 2 – Ausnahmen vom Anwendungsbereich (4/5)

Wissenschaftliche Forschung und Entwicklung:

- **Text nach politischer Einigung:**

Art 2 (6):

This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

Art 2 (8):

This Regulation does not apply to any research, testing or and development activity regarding AI systems or AI models prior to their being placed on the market or put into service. Such activities shall be conducted respecting in accordance with applicable Union law. Testing in real world conditions shall not be covered by that exclusion.

Art 2 – Ausnahmen vom Anwendungsbereich (5/5)

Open source:

- **EK-Vorschlag / Allgemeine Ausrichtung:**

Keine entsprechende Regelung.

- **Text nach politischer Einigung:**

Art 2 (12):

This Regulation does not apply to AI systems released under free and open-source licences, unless they are placed on the market or put into service as high-risk AI systems or as an AI system that falls under Article 5 or 50.

Art 3 Z 1 Definition eines KI-Systems

- **EK-Vorschlag:**

‘artificial intelligence system’ (AI system) means 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;

- **Allgemeine Ausrichtung:**

‘artificial intelligence system’ (AI system) means a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts;

- **Text nach politischer Einigung:**

‘AI system‘ means 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;

Art 5 Verbotene Praktiken

- **EK-Vorschlag / Allgemeine Ausrichtung / Text nach politischer Einigung**

1. […]

(h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces (~~by law enforcement authorities or on their behalf~~) for the purpose of law enforcement unless and in as far as such use is strictly necessary for one of the following objectives:

(i) the targeted search for specific victims of abduction, trafficking in human beings and sexual exploitation of human beings as well as search for missing persons (~~potential victims of crime~~), ~~including missing children~~;

(ii) the prevention of a specific, substantial and imminent threat to the (~~critical infrastructure,~~) life or physical safety of natural persons or (~~the prevention~~) a genuine and present or genuine and foreseeable threat of a terrorist attack;

(iii) the (~~detection,~~) localisation~~,~~ or identification (~~or prosecution~~) of a (~~perpetrator~~) (~~natural~~) person suspected of having committed a criminal offence, for the purposes of conducting a criminal investigation, prosecution or executing a criminal penalty for (~~or suspect of a criminal~~) offences, referred to in (~~Article 2(2) of Council Framework Decision 2002/584/JHA62~~) Annex IIa and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least (~~three~~) four years.~~,~~ (~~or other specific offences punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least five years, as determined by the law of that Member State.~~) This paragraph is without prejudice to the provisions in Article 9 of the GDPR for the processing of biometric data for purposes other than law enforcement.

Art 5 Verbotene Praktiken

- **EK-Vorschlag / Allgemeine Ausrichtung / Text nach politischer Einigung**

2. The use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point h) shall be deployed for the purposes set out in paragraph 1, point (h), only to confirm the identity of the specifically targeted individual and it shall take into account the following elements:

(a) the nature of the situation giving rise to the possible use, in particular the seriousness, probability and scale of the harm caused in the absence of the use of the system;

(b) the consequences of the use of the system for the rights and freedoms of all persons concerned, in particular the seriousness, probability and scale of those consequences.

In addition, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement for any of the objectives referred to in paragraph 1 point d) shall comply with necessary and proportionate safeguards and conditions in relation to the use in accordance with national legislations authorizing the use thereof, in particular as regards the temporal, geographic and personal limitations. The use of the 'real-time' remote biometric identification system in publicly accessible spaces shall only be authorised if the law enforcement authority has completed a fundamental rights impact assessment as provided for in Article 27 and has registered the system in the database according to Article 49. However, in duly justified cases of urgency, the use of such systems may be commenced without the registration in the EU database, provided that such registration is completed without undue delay.

Art 5 Verbotene Praktiken

- **EK-Vorschlag / Allgemeine Ausrichtung / Text nach politischer Einigung**

3. For the purposes of paragraphs 1, point (h) and 2, each individual use for the purpose of law enforcement of a 'real-time' remote biometric identification system in publicly accessible spaces shall be subject to a prior authorisation granted by a judicial authority or by an independent administrative authority whose decision is binding of the Member State in which the use is to take place, issued upon a reasoned request and in accordance with the detailed rules of national law referred to in paragraph 5. However, in a duly justified situation of urgency, the use of such system may be commenced without an authorisation provided that, such authorisation (~~shall be~~) is requested without undue delay, at the latest within 24 hours. (~~during use of the AI system, and)~~ If such authorisation is rejected, its use shall be stopped with immediate effect and all the data, as well as the results and outputs of that use shall be immediately discarded and deleted. ~~and the authorisation may be requested only during or after the use~~.

The competent judicial or independent administrative authority whose decision is binding shall only grant the authorisation where it is satisfied, based on objective evidence or clear indications presented to it, that the use of the 'real-time' remote biometric identification system at issue is necessary for and proportionate to achieving one of the objectives specified in paragraph 1, point (d), as identified in the request and, in particular, remains limited to what is strictly necessary concerning the period of time as well as geographic and personal scope. In deciding on the request, that authority shall take into account the elements referred to in paragraph 2. It shall be ensured that no decision that produces an adverse legal effect on a person may be taken by that authority solely based on the output of the 'real-time' remote biometric identification system.

Art 5 Verbotene Praktiken

- **EK-Vorschlag / Allgemeine Ausrichtung / Text nach politischer Einigung**

4. Without prejudice to paragraph 3, each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes shall be notified to the relevant market surveillance authority and the national data protection authority in accordance with the national rules referred to in paragraph 5. The notification shall as a minimum contain the information specified under paragraph 6 and shall not include sensitive operational data.

5. A Member State may decide to provide for the possibility to fully or partially authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within the limits and under the conditions listed in paragraphs 1, point (h), 2 and 3. That Member State shall lay down in its national law the necessary detailed rules for the request, issuance and exercise of, as well as supervision relating to, the authorisations referred to in paragraph 3. Those rules shall also specify in respect of which of the objectives listed in paragraph 1, point (h), including which of the criminal offences referred to in point (h) (iii) thereof, the competent authorities may be authorised to use those systems for the purposes of law enforcement. Member States shall notify those rules to the Commission at the latest 30 days following the adoption thereof. Member States may introduce, in accordance with Union law, more restrictive laws on the use of remote biometric identification systems.

Art 5 Verbotene Praktiken

- **Text nach politischer Einigung**

6. National market surveillance authorities and the national data protection authorities of Member States that have been notified of the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes pursuant to paragraph 4 shall submit to the Commission annual reports on such use. For that purpose, the Commission shall provide Member States and national market surveillance and data protection authorities with a template, including information on the number of the decisions taken by competent judicial authorities or an independent administrative authority whose decision is binding upon requests for authorisations in accordance with paragraph 3 and their result.

7. The Commission shall publish annual reports on the use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes based on aggregated data in Member States based on the annual reports referred to in paragraph 6, which shall not include sensitive operational data of the related law enforcement activities.

Art 6 Klassifizierung von HR-KI-Systemen

- **EK Vorschlag / Allgemeine Ausrichtung**

[…]

(2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk).

3. AI systems referred to in Annex III shall be considered high-risk unless the output of the system is purely accessory in respect of the relevant action or decision to be taken and is not therefore likely to lead to a significant risk to the health, safety or fundamental rights.

In order to ensure uniform conditions for the implementation of this Regulation, the Commission shall, no later than one year after the entry into force of this Regulation, adopt implementing acts to specify the circumstances where the output of AI systems referred to in Annex III would be purely accessory in respect of the relevant action or decision to be taken. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 74, paragraph 2.

Art 6 Klassifizierung von HR-KI-Systemen

- **Text nach politischer Einigung**

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

3. By derogation from paragraph 2 an AI system referred to in Annex III shall not be considered to be high risk where they do not pose a significant risk of harm, to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.

The first subparagraph shall be the case where one or more of the following conditions are fulfilled:
(a) the AI system is intended to perform a narrow procedural task;
(b) the AI system is intended to improve the result of a previously completed human activity;
(c) the AI system is intended to 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; or
(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be high-risk if the AI system performs profiling of natural persons.

4. A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.

Art 6 Klassifizierung von HR-KI-Systemen

- **Text nach politischer Einigung**

5. The Commission shall, after consulting the AI Board, and no later than 18 months from the date of the entry into force of this Regulation, provide guidelines specifying the practical implementation of this article in line with Article 96 together with a comprehensive list of practical examples of use cases of AI systems that are high risk and not high risk.

6. The Commission is empowered to adopt delegated acts in accordance with Article 97 in order to amend paragraph 3, second subparagraph, of this Article by adding new criteria conditions to those laid down there or modifying them, where there is concrete and reliable evidence of the existence of AI systems that fall under the scope of Annex III but that do not pose a significant risk of harm to the health, safety and fundamental rights of natural persons.

7. The Commission shall adopt delegated acts in accordance with Article 97 in order to amend paragraph 3, second subparagraph, of this Article by deleting any of the conditions laid down there, where there is concrete and reliable evidence that this is necessary to maintain the level of protection of health, safety and fundamental rights in the Union provided for by this Regulation.

[…]

Anhang III Liste der HR-KI-Anwendungen

- **EK Vorschlag / Allgemeine Ausrichtung / Text nach politischer Einigung**

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;

1. Biometrics

(a) Remote biometric identification systems

1. Biometrics, insofar as their use is permitted under relevant Union or national law:

(a) remote biometric identification systems.

This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;

(b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;

(c) AI systems intended to be used for emotion recognition.

Anhang III Liste der HR-KI-Anwendungen

- **Neue Anwendungsfälle (Auszug)**

5. *[…]*

(c) *AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.*

7. *[…]*

(d) *AI systems intended to be used by or on behalf of competent public authorities, including Union agencies, offices or bodies, in the context of migration, asylum and border control management, for the purpose of detecting, recognising or identifying natural persons with the exception of verification of travel documents.*

8. *[…]*

(b) *AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view.*

KI-Systeme mit allgemeinem Verwendungszweck / Basismodelle

Allgemeine Ausrichtung

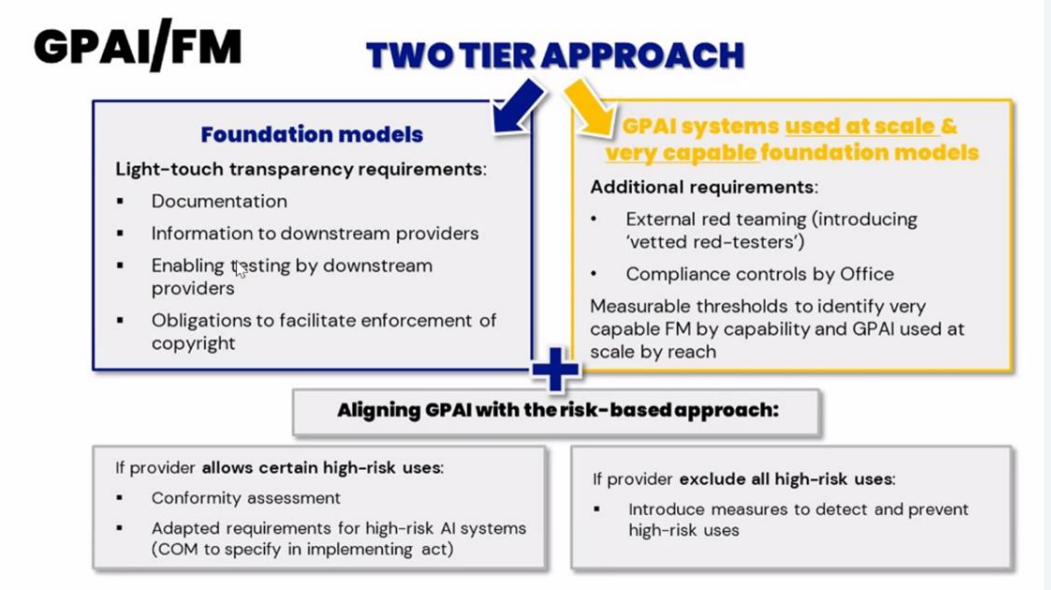
(Art 4a, 4b, 4c - Zusammenfassung)

Unbeschadet der Art 5, 52, 53 und 69 müssen KI-Systeme mit allgemeinem Verwendungszweck lediglich die Anforderungen und Verpflichtungen nach Art 4b erfüllen.

Anforderungen für Allzweck-KI-Systeme werden gem Art 4b in einen DfRA ausgestaltet (dh keine direkte Anwendbarkeit der Anforderungen). Dem vorangehen soll eine Konsultation, Folgenabschätzung und es sollen auch die spezifischen Merkmale dieser Systeme etc berücksichtigt werden.

Art 4b gilt nicht, wenn der Anbieter in den Gebrauchsanweisungen oder in den Begleitdokumenten des KI-Systems mit allgemeinem Verwendungszweck ausdrücklich jegliche Verwendung mit hohem Risiko ausgeschlossen hat.

Nach politischer Einigung



State of play – „Gesetz über künstliche Intelligenz“

- Am 8.12.2023 politische Einigung zwischen den Ko-Gesetzgebern
- Knackpunkte der Trilogverhandlungen:
  - Art 2 Abs 3: Ausnahme für nationale Sicherheit vom Anwendungsbereich
  - Art 5 Verbotene Praktiken
  - Art 6 Klassifizierung von HR-KI-Systemen / Annex III
  - KI-Systeme mit allgemeinem Verwendungszweck / Basismodelle
  - Governance/Durchsetzungsbehörden
- Abstimmung im EP Plenum am 13.3.2024 erfolgt (EN Sprachfassung)
- Derzeit sprachjuristische Überarbeitung

Nächste Schritte

- **EP Plenarwoche von 22.-25.4.:** EP-Annahme des finalen Texts (ohne Abstimmung – Corrigendum / Sprachfassungen)
- **Ende April:** Annahme im AStV als I-Punkt (Datum noch tbc)
- **Mai:** Annahme im Rat als A-Punkt in den ersten beiden Maiwochen (Rat noch tbd)
- **Juni:** Veröffentlichung im EU-Amtsblatt und Inkrafttreten (20 Tage danach)
- Fristenlauf beginnt mit Zeitpunkt des Inkrafttretens (sh. Grafik auf nächster Folie)

Umsetzungsfristen

6 Monate

Verbote von KI-Systemen mit unannehmbaren Risiken

9 Monate

Codes of Practice

12 Monate

Verpflichtungen für Anbieter von GPAI

Benennung der zuständigen Behörden in den MS

Strafen

Jährliche Überprüfung (und möglich Ergänzungen) der Liste der verbotenen KI-Systeme durch die EK

18 Monate

Durchführungsrechtsakt für Marktüberwachung nach dem Inverkehrbringen

24 Monate

Verpflichtungen für HR-KI-Systeme aus Annex III

mind. 1 Regulatory Sandbox

36 Monate

Verpflichtungen für HR-KI-Systeme, gem. Artikel 6 (1), die als Sicherheitskomponente eines Produkts verwendet werden sollen, oder das KI-System selbst ist ein Produkt, und das Produkt muss einer Konformitätsbewertung durch einen Dritten unterzogen werden

Vergleich der vorhandenen Stellen in EU und AT

Anforderungen an die nationale Umsetzung des AI Acts

Fragen?

Vielen Dank!

Kontakt:
Julia FUITH
julia.fuith@bmf.gv.at