Acting as the voice of the **security industry**

Confederation of European Security Services

CoESS CHARTA über den ethischen und verantwortungsvollen Einsatz von **Künstlicher Intelligenz** in den europäischen privaten Sicherheitsdienstleistungsunternehmen

BDSW
BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

VSÖ
VERBAND DER SICHERHEITSUNTERNEHMEN ÖSTERREICHS

VSSU

11 Oktober 2024

Haftungsausschluss:

Diese Charta wurde von einer speziellen Expertengruppe der CoESS für die europäische private Sicherheitsindustrie entwickelt. Sie konzentriert sich ausschließlich auf Leitlinien für Betreiber von KI-Systemen.

Dieses Dokument soll Sicherheitsdienstleistungsunternehmen ein erstes Verständnis des EU-KI-Gesetzes und wichtiger Verhaltenskodizes vor und während der Nutzung eines KI-Systems vermitteln. Die Informationen in dieser Charta ersetzen nicht die spezifischen Risiko- und Regulierungsbewertungen für Systeme und Anwendungsfälle, die vom Betreiber durchgeführt werden müssen, um die Einhaltung des EU-KI-Gesetzes sicherzustellen.

Design & graphics:
https://blog.acapella.be/

Photo credits:
© AdobeStock: 713733409: Milan, 913052673*: suratin, 874669432*: Andres Mejia, 588772865: NicoElNino, 846542130*: ImageFlow, 802446835*: ERiK, 728100169*: Miumzlik, 355680792 and 516647240: .shock, 794014906*: Natanong, 720464800*: inthasone, 725689364*: sandsun, 777449543*: Bartek, 185898613: Kadmy, 732479109*: ALL YOU NEED studio, 861484312*: ALEXSTUDIO, 824935213: pressmaster, 326350464: PX Media
* *Generated with AI*

© iStock: 2130201321: Suriya Phosri, 1472578503: Pakpoom Makpan, 1428421517: Galeanu Mihai, 1168365129: metamorworks

Besonderer Dank an die aktiven Mitwirkenden an dieser Charta (alphabetisch geordnet):

Carolina Garcia Cortés, Innovationsmanagerin, Prosegur
Cornelius Toussaint, CEO, Condor Group
Daniel Sandberg, Direktor für Künstliche Intelligenz, Securitas Group
Graham Evans, Technischer Berater, BSIA
Helena Eriksvik, Leiterin der globalen Abteilung für Recht, Daten & Datenschutz, Securitas Group
Pauline Norstrom, CEO Anekanta®AI und Vertreterin des BSIA
Victoria Ferrera Lopez, Senior Managerin für regulatorische Angelegenheiten, Verisure
Wim Bartsoen, Chief Digital Security Officer, Securitas Group

Über die CoESS:

Der Verband der Europäischen Sicherheitsdienstleistungsunternehmen (CoESS) ist die Stimme der privaten Sicherheitsindustrie in Europa und deckt 22 Länder ab. Die CoESS vertritt 45.000 Unternehmen mit 2 Millionen Sicherheitskräften. Private Sicherheitsdienste bieten eine breite Palette an Dienstleistungen, sowohl für private als auch öffentliche Auftraggeber, für kritische Infrastrukturen und öffentliche Räume und Lieferketten bis hin zu staatlichen Einrichtungen an. Die CoESS wird von der Europäischen Kommission als Vertretung der europäischen Arbeitgeberorganisation anerkannt. Wir sind aktiv im europäischen sektoralen Sozialdialog sowie in mehreren EU-Expertengruppen tätig – einschließlich SAGAS, SAGMAS, LANDSEC, dem EU Operators Forum zum Schutz öffentlicher Räume und der EU Ports Alliance.
EU-Transparenzregister-Nummer: 61991787780-18

Zusammenfassung

Diese Charta, die im Einklang mit dem EU-Gesetz über Künstliche Intelligenz (KI) und den Kernwerten der CoESS entwickelt wurde, legt einen Rahmen über **zehn wesentliche Anforderungen** für den **verantwortungsvollen und ethischen Einsatz von Künstlicher Intelligenz (KI)** durch europäische Sicherheitsdienstleistungsunternehmen fest.

1. **RISIKOMANAGEMENT:** Ergreifen Sie geeignete und gezielte Risikomanagement-maßnahmen.
2. **DATENVERWALTUNG:** Stellen Sie eine sorgfältige Datenverwaltung sicher, die die Nutzung vertrauenswürdiger Daten und die strikte Einhaltung der Datenschutz-Grundverordnung (DSGVO) gewährleistet.
3. **MENSCHLICHE AUFSICHT:** Statten Sie das Personal mit der notwendigen Schulung und den entsprechenden Richtlinien aus, um die Anforderungen an die menschliche Aufsicht zu erfüllen, und zwar in Übereinstimmung mit dem spezifischen KI-Anwendungsfall.
4. **RESILIENZ-MASSNAHMEN:** Erreichen Sie einen robusten physischen und cybertechnischen Schutz für Unternehmenswerte, KI-Systeme und die zugehörige Infrastruktur.
5. **DOKUMENTATION:** Dokumentieren Sie die Leistungsfähigkeit der KI-Systeme im Betrieb.
6. **TRANSPARENZ UND NACHVOLLZIEHBARKEIT:** Setzen Sie geeignete Transparenzmaßnahmen um, die die Einhaltung der DSGVO und des EU-KI-Gesetzes gewährleisten und erzielen Sie ein angemessenes Maß an Nachvollziehbarkeit.
7. **BEWERTUNG DER AUSWIRKUNGEN AUF DIE GRUNDRECHTE:** Führen Sie Bewertungen zu den möglichen Auswirkungen auf die Grundrechte durch, auch wenn dies keine gesetzliche Verpflichtung ist, jedoch Bedenken hinsichtlich möglicher, wenn auch unwahrscheinlicher, Auswirkungen auf die Rechte bestehen.
8. **SORGFALTSPFLICHT:** Befolgen Sie Sorgfaltspflichtrichtlinien beim Erwerb von KI-Systemen.
9. **EINBINDUNG DER ARBEITNEHMER:** Fördern Sie das Bewusstsein der Arbeitnehmer über den Einsatz von KI in Ihrem Unternehmen und setzen Sie Mechanismen zur Adressierung von Bedenken um, insbesondere bei der Nutzung von KI mit hohem Risiko.
10. **ZUSAMMENARBEIT MIT DEN BEHÖRDEN:** Arbeiten Sie aktiv mit den zuständigen Behörden zusammen, um zusätzliche Leitlinien zu erhalten und rechtliche Unsicherheiten sowie Anforderungen zur Einhaltung der Vorschriften zu klären.

INHALTSVERZEICHNIS

Einleitung

Die Integration von Künstlicher Intelligenz (KI) in Sicherheitsdienstleistungen wird voraussichtlich eine wichtige Rolle, in der sich ständig weiterentwickelnden Transformation der Sicherheitsbranche spielen.

Von datengestützter Risikoanalyse bis hin zu integrierter Videoüberwachung können KI-Systeme in vielen verschiedenen Anwendungsfällen in Sicherheitsdienstleistungen eingesetzt werden, wodurch Vorteile für Mitarbeiter, Kunden, Unternehmen und die öffentliche Sicherheit entstehen. Dennoch gibt es bei einigen Anwendungsfällen auch Risiken.

Die Europäische Union (EU) hat daher die Entwicklung und den Einsatz sogenannter „hochrisikobehafteter" KI im EU-KI-Gesetz geregelt. Sicherheitsdienstleistungsunternehmen, die in der EU tätig sind und KI-Systeme in ihre Dienstleistungen integrieren, müssen ab dem 2. August 2026 mit den meisten Aspekten des Gesetzes in Einklang stehen, wobei einige Bestimmungen bereits ab dem 2. Februar 2025 gelten. Es ist wichtig, Unternehmen zu helfen, die Auswirkungen des EU-KI-Gesetzes auf ihre Geschäftstätigkeit zu verstehen. Viele Unternehmen sind sich möglicherweise noch nicht einmal bewusst, ob sie KI in ihren Dienstleistungen einsetzen. Aber ab jetzt muss jedes Sicherheitsdienstleistungsunternehmen, groß oder klein, wissen, ob es ein KI-System einsetzt und was zu tun ist. Aber es gibt weitere Aspekte.

Der Verband der Europäischen Sicherheit-Dienstleistungs-Unternehmen (CoESS) und ihre Mitglieder stehen für eine menschenzentrierte Innovation für das Gemeinwohl und ein unerschütterliches Bekenntnis zu Ethik, Verantwortung und Compliance.

Zeitleiste : Anwendung des EU-KI-Gesetzes

Diese Charta soll daher nicht nur den Unternehmen helfen, mit dem EU-KI-Gesetz in Einklang zu kommen, sondern auch KI-Systeme auf verantwortungsvolle und ethische Weise zu integrieren, die über die bloße Einhaltung hinausgeht. Zu diesem Zweck ist diese Charta in vier Kapitel unterteilt:

- KAPITEL I gibt Unternehmen eine Orientierungshilfe, um KI-Systeme und „hochrisikobehaftete" Anwendungsfälle in Sicherheitsdienstleistungen auf Grundlage rechtlicher und anderer übergreifender Kriterien zu identifizieren.
- KAPITEL II bietet einen Überblick über Chancen und Risiken, die mit dem Einsatz von KI in Sicherheitsdienstleistungen verbunden sind.
- KAPITEL III legt Anforderungen für die Anbieter von KI im Sicherheitssektor fest, die relevante Risiken ansprechen, sowohl im Hinblick auf die gesetzlichen Verpflichtungen des EU-KI-Gesetzes als auch auf die Werte der CoESS.
- KAPITEL IV enthält eine leicht verständliche Checkliste für Unternehmen zu den Schritten, die beim Planen der Bereitstellung eines KI-Systems heute zu unternehmen sind.

HAFTUNGSAUSSCHLUSS

Diese Charta wurde von einer eigens eingerichteten Expertengruppe der CoESS für die europäische Privatwirtschaft im Sicherheitssektor entwickelt. Sie richtet sich ausschließlich an Anbieter von KI-Systemen.

Dieses Dokument soll Sicherheitsdienstleistungsunternehmen ein erstes Verständnis des EU-KI-Gesetzes und wichtiger Verhaltensrichtlinien vor und während der Nutzung eines KI-Systems vermitteln. Die in dieser Charta enthaltenen Informationen ersetzen nicht die system- und anwendungsspezifischen Risiko- und Regulierungsbewertungen, die vom Anbieter durchgeführt werden sollten, um die Einhaltung des EU-KI-Gesetzes sicherzustellen.

Kapitel I: Definition von KI und Anwendungsfälle in Europäischen Sicherheitsdienstleistungsunternehmen

I. Was ist KI? Auf der Suche nach einer Definition

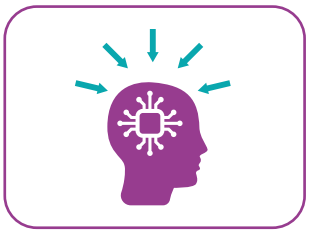
Die erste Frage, die sich jeder Anwender stellen muss, lautet: Nutze ich KI? Die rechtliche Definition von KI ist jedoch ein komplexes Thema mit unterschiedlichen Ansätzen weltweit. Diese Charta fördert insbesondere die Einhaltung des EU-KI-Gesetzes, daher beziehen wir uns in diesem Dokument auf die KI-Definition im EU-Recht.

Im EU-KI-Gesetz stimmt die EU die rechtliche Definition von KI stark mit der der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ab. Laut Artikel 3.1 des EU-KI-Gesetzes wird ein KI-System wie folgt definiert:

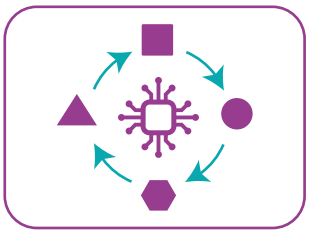
> *„KI-System": ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie betrieben werden kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ausgaben wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen generieren kann, die physische oder virtuelle Umgebungen beeinflussen können.*

Diese rechtliche Definition ist in der Tat komplex. Es ist daher hilfreich, einen Blick auf die OECD-KI-Prinzipien[1], einen intergouvernementalen Standard für KI, zu werfen und die verschiedenen Aspekte zu erklären:

VERSCHIEDENE AUTONOMIESTUFEN[2]: Ein KI-System kann eine Aufgabe mit unterschiedlicher menschlicher Unterstützung erfüllen, von teilweise bis vollständig autonom. Dies ist sowohl der Hauptvorteil als auch das Risiko im Zusammenhang mit dem Einsatz von KI. Je nach Ergebnis der Aufgabe und dem Grad der menschlichen Aufsicht können selbst einfache, vollständig autonome Systeme ein erhebliches Risiko für grundlegende Rechte darstellen.



ANPASSUNGSFÄHIGKEIT: Ein weiteres zentrales Merkmal – aber auch Risiko – vieler KI-Systeme ist ihre Fähigkeit, selbst zu lernen und sich anzupassen oder zu entwickeln. Sie entwickeln sich auf Basis von Eingaben der Nutzer, das heißt, nach der Design- und Bereitstellungsphase. KI birgt daher ein inhärentes Risiko, dass das System Daten auf eine Weise verarbeitet, die oft als „Blackbox" bezeichnet wird, was die Erklärbarkeit der Ergebnisse des KI-Systems verringern kann.

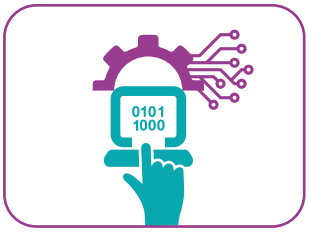


[1] *R. Stuart, K. Perset, M. Grobelnik (2023): Updates to the OECD's definition of an AI system explained. Available here: https://oecd.ai/en/wonk/ai-system-definition-update*

[2] *Zusätzliche Referenzen zur Definition von Autonomie in KI-Systemen: EN ISO/IEC 22989 und Erwägungsgrund 12 der EU-KI-Verordnung: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf*

EXPLIZITE UND IMPLIZITE ZIELE: Ein KI-System kann unterschiedliche Ziele haben. Explizite Ziele sind in der Regel das Ergebnis der von den Entwicklern (und möglicherweise auch den Betreibern) festgelegten Regeln – z. B. ein Drohnensystem, das autonom ein Objekt von A nach B transportiert. Es gibt jedoch auch KI-Systeme, die nur implizite Ziele haben, wie etwa KI für allgemeine Zwecke, die auf großen Sprachmodellen (LLM) basiert.

EINGABE: KI-Systeme basieren auf Eingabedaten, die notwendig sind, damit sie eine Ausgabe generieren können. Die Eingabe kann aus Regelwerken und Algorithmen bestehen, die vom Entwickler festgelegt wurden, Trainingsdaten, die der Entwickler verwendet, um das KI-System weiterzuentwickeln, zusätzlichen Anweisungen des Betreibers und Daten aus der Umwelt, die zur Selbstlernfähigkeit des Systems beitragen können.



AUSGABE: Der Entwickler (und gegebenenfalls auch die Betreiber des Systems) bestimmt die beabsichtigten Funktionen des KI-Systems sowie die Arten von Ausgaben, die es generieren wird – wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen. Um eine Ausgabe zu erzeugen, verarbeitet das KI-System seine Eingaben auf Grundlage von Regeln, Anweisungen und Algorithmen, die von den Entwicklern erstellt und gegebenenfalls von den Betreibern weiter verfeinert wurden. Hochrisiko-Anwendungen beinhalten typischerweise Ausgaben, die erhebliche Auswirkungen auf die reale Welt haben und mit einem hohen Automatisierungsgrad arbeiten, wodurch nur wenig menschliche Aufsicht verbleibt.

UMGEBUNG: Umgebungen, die die KI-Systeme mit Eingaben versorgen und denen die Ausgaben unterliegen, können sowohl physisch (z. B. die Erkennung und Verifizierung von Objekten und natürlichen Personen) als auch virtuell (z. B. bei der Analyse von Geschäftsprozessen) sein.

II. Die Verwendung von übergreifenden Kriterien zur Unterscheidung zwischen niedrig- und hochriskanten KI-Systemen

Die verschiedenen Aspekte, die das Funktionieren von KI-Systemen erklären können, lassen sich auch als miteinander verbundene, übergreifende Kriterien verwenden, die dem Betreiber eine erste Orientierung bieten können, um:

- → zu erkennen, ob ein System selbst ein KI-Produkt oder ein KI-Sicherheitsbaustein eines Produkts ist.
- → zwischen niedrig- und hochriskanten KI-Systemen und Anwendungsfällen zu unterscheiden.

Jede Bewertung eines KI-Systems und Anwendungsfalls ist jedoch einzigartig und unterliegt innerhalb der EU der Definition von niedrig- und hochriskanter KI im EU-KI-Gesetz.

Ein weiterer, umfassenderer Ansatz zur Definition verschiedener Kriterien und Merkmale von KI ist in der EN ISO/IEC Norm 23053:2022 (Rahmenwerk für Künstliche Intelligenz Systeme unter Verwendung von Maschinellem Lernen) zu finden.

„Jede Bewertung eines KI-Systems und Anwendungsfalls ist jedoch einzigartig“

AUTONOMIE

Wenn das KI-System autonome Ausgaben in einer physischen Umgebung erzeugt, ist es wahrscheinlich, dass es als hochriskant eingestuft wird. Das EU-KI-Gesetz macht daher die menschliche Aufsicht für hochriskante KI-Systeme und Anwendungsfälle obligatorisch.

ADAPTIVITÄT

Wenn der Entscheidungsprozess des KI-Systems auf logischem Selbstlernen in einer „Blackbox“ basiert und sich im Laufe der Zeit weiterentwickelt, kann dies zu einer erhöhten mangelnden Erklärbarkeit führen, was das System eher als hochriskant klassifizieren lässt.

ZIELE

Wenn die Ziele des KI-Systems Auswirkungen auf natürliche Personen haben oder implizit sind, wird es wahrscheinlicher, dass das KI-System und der Anwendungsfall als hochriskant eingestuft werden.

EINGABE

Wenn die Eingabe auf personenbezogenen Daten natürlicher Personen basiert, ist die Einhaltung der DSGVO entscheidend und das Risiko als hochriskant eingestuft zu werden steigt.

AUSGABE

Wenn die Ausgabe des KI-Systems ein Risiko für die Gesundheit, Sicherheit oder die Grundrechte natürlicher Personen darstellt, einschließlich der wesentlichen Beeinflussung des Ergebnisses eines Entscheidungsprozesses, ist es wahrscheinlich, dass das System als hochriskant eingestuft wird.

UMGEBUNG

Wenn die Ausgabe eine Umgebung betrifft, die eine natürliche Person einschließt, steigt die Wahrscheinlichkeit, dass das KI-System und der Anwendungsfall als hochriskant eingestuft werden.

III. Das EU-KI-Gesetz und rechtliche Compliance: Niedrigrisiko vs. Hochrisiko KI

Verschiedene KI-Systeme und Anwendungsfälle bergen unterschiedliche Risiken. Das EU-KI-Gesetz folgt einem risikobasierten Ansatz und regelt hauptsächlich hochriskante KI-Systeme und Anwendungsfälle. In diesem Kapitel möchten wir den Anwendern von KI-Systemen in der europäischen privaten Sicherheitsbranche ein erstes Verständnis des Ansatzes des EU-KI-Gesetzes vermitteln. Bitte beachten Sie, dass zu erwarten ist, dass das EU-KI-Büro der Europäischen Kommission, Leitlinien zur Definition von KI-Systemen, Verboten und der Hochrisiko-Klassifikation entwickeln wird.

Zu Beginn: Jeder Anbieter und Nutzer von KI-Systemen muss das EU-KI-Gesetz einhalten.

Das ist jedoch der einzige einfache Teil. Denn die rechtlichen Verpflichtungen für die Anwender von KI-Systemen (siehe ab Seite 27) unterscheiden sich je nach Risiko des jeweiligen Systems und Anwendungsfalls. Das EU-KI-Gesetz unterscheidet zwischen den folgenden Kategorien von KI-Systemen und Anwendungsfällen:

1. NIEDRIGRISIKO KI-SYSTEME UND ANWENDUNGSFÄLLE
2. VERBOTENE KI-PRAKTIKEN
3. HOCHRISIKO KI-SYSTEME UND ANWENDUNGSFÄLLE

1. Niedrigrisiko KI

Niedrigrisiko sind allgemein die KI-Systeme und Anwendungsfälle, die nicht in die Kategorien „verboten“ und „Hochrisiko“ fallen. Das EU-KI-Gesetz präzisiert weiter in Artikel 6.3, dass ein KI-System auch dann allgemein als Niedrigrisiko klassifiziert wird, wenn es dazu bestimmt ist:

- eine eng begrenzte verfahrensorientierte Aufgabe oder eine bloße Vorbereitungsaufgabe von Hochrisiko KI-Anwendungsfällen zu erfüllen
- das Ergebnis einer zuvor durchgeführten menschlichen Tätigkeit zu verbessern
- die zuvor durchgeführte menschliche Beurteilung nur unter ordnungsgemäßer menschlicher Überprüfung zu ersetzen oder zu beeinflussen.

Innerhalb der Niedrigrisiko-Kategorie unterscheidet der EU-KI-Gesetz weiter zwischen Systemen mit minimalem Risiko, für die keine rechtlichen Verpflichtungen bestehen, und bestimmten KI-Systemen mit einem Transparenzrisiko, die bestimmten Transparenzverpflichtungen nachkommen müssen.[3]

„Jeder Anbieter und Nutzer von KI-Systemen muss das EU-KI-Gesetz einhalten“

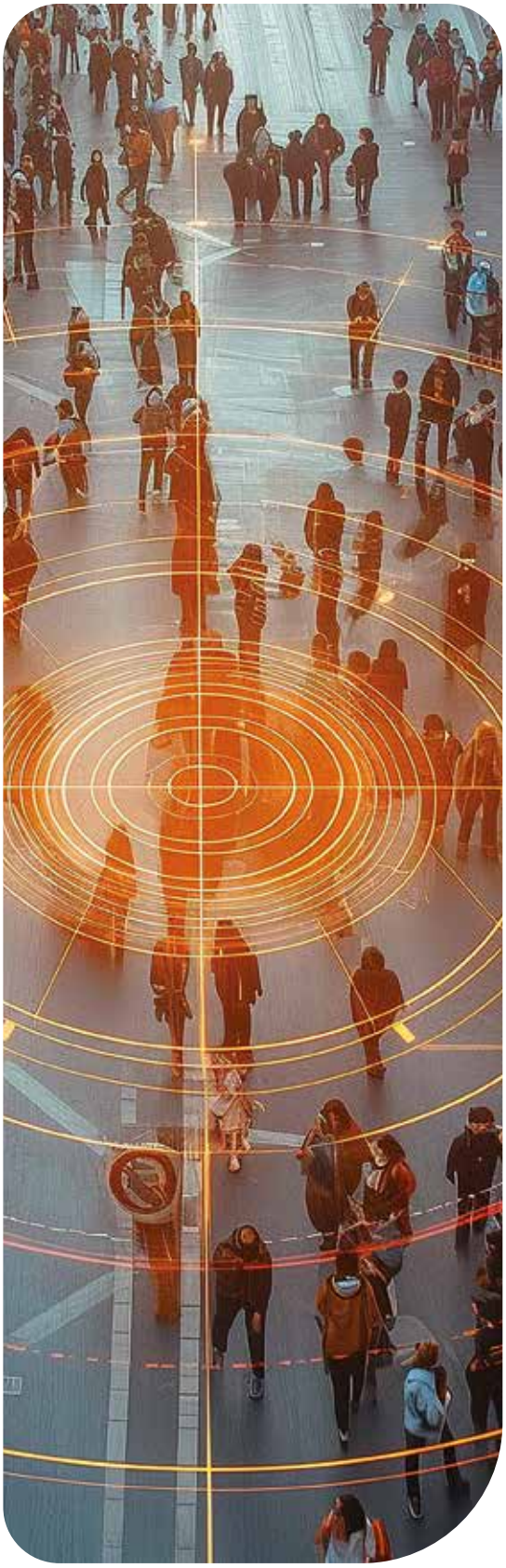
[3] *KI-Systeme, die mit natürlichen Personen interagieren, aber als Niedrigrisiko eingestuft werden (wie zum Beispiel LLMs und Chatbots), müssen bestimmte Transparenzpflichten erfüllen, die in Artikel 50 des EU-KI-Gesetzes festgelegt sind. Zum Beispiel muss die betroffene natürliche Person darüber informiert werden, dass sie mit einem KI-System interagiert. Alle KI-Systeme, die weder verboten noch als „Hochrisiko“ eingestuft werden (siehe Seite 13) oder Systeme mit einem Transparenzrisiko sind, gelten als minimalrisikobehaftet. Die Anwender solcher Systeme müssen nicht den umfangreichen rechtlichen Verpflichtungen des EU-KI-Gesetzes nachkommen, werden jedoch ermutigt, freiwillige Verhaltenskodizes anzuwenden – die von EU-Gremien, Mitgliedstaaten oder Vertretungsorganisationen entwickelt werden sollen.*

2. Verbotene KI-Praktiken

Das EU-KI-Gesetz definiert in Artikel 5 jene KI-Systeme und Anwendungsfälle, die ein inakzeptables Risiko für die Grundrechte der europäischen Bürger darstellen. Diese sind daher verboten und dürfen ab dem 02. Februar 2025 weder vermarktet noch in der EU genutzt werden. Dazu gehören:

- *Profiling zur Einschätzung oder Vorhersage des Risikos, dass eine Person ein Verbrechen begeht*
- *Erstellung von Gesichtserkennungs-Datenbanken durch automatisierte Bildsuchen auf CCTV oder im Internet*
- *Soziales Scoring, das zu nachteiliger Behandlung von natürlichen Personen führt*
- *Biometrische Kategorisierung von unrechtmäßig erfassten Datensätzen*
- *Echtzeit-ferngesteuerte biometrische Identifikation in öffentlichen Räumen, wie der Einsatz von Gesichtserkennungstechnologie (FRT), mit wichtigen Ausnahmen im Bereich der Strafverfolgung*[4]
- *Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen (außer bei Verwendung zu medizinischen und Sicherheitszwecken).*

Das EU-KI-Büro wird weitere Leitlinien zur Definition von KI-Systemen und Verboten veröffentlichen.



[4] *Es gibt Ausnahmen für die Nutzung von Echtzeit-Fernbiometrie-Identifikationssystemen in öffentlich zugänglichen Bereichen durch Strafverfolgungsbehörden oder in deren Auftrag. Diese Systeme identifizieren automatisch eine natürliche Person ohne deren Zustimmung. Mitgliedstaaten können die Verwendung solcher Technologien in öffentlichen Räumen vollständig oder teilweise gestatten, innerhalb der im EU-KI-Gesetzes festgelegten Grenzen (z. B. gerichtliche Genehmigungen), wenn sie für die gezielte Suche nach einem Entführungsopfer oder einer Person, die des Verdachts auf eine Straftat (wie in Anhang II des EU KI- Gesetzes definiert) unterliegt, sowie zur Prävention einer spezifischen, erheblichen und unmittelbaren Bedrohung des Lebens oder der physischen Sicherheit von Bürgern, wie etwa einem Terroranschlag, eingesetzt werden. Mitgliedstaaten können jedoch auch strengere Regelungen festlegen. Daher kann die Regulierung von einem Mitgliedstaat der EU zum anderen unterschiedlich ausfallen.*

3. Hochrisiko KI

Dies ist die wichtigste Kategorie, da das EU-KI-Gesetz Regeln für den Einsatz von hochriskanten KI-Systemen definiert.

„Das EU-KI-Gesetz Regeln für den Einsatz von hochriskanten KI-Systemen definiert“

Sobald der Anwender festgestellt hat, ob ein KI-System verwendet wird, ist es wichtig zu bewerten, ob es gemäß der Definition des EU-KI-Gesetzes in Artikel 6 als Hochrisiko eingestuft wird:

1. Das KI-System ist ein Produkt oder eine Sicherheitskomponente eines Produkts, das (1) von bestehender Gesetzgebung gemäß Anhang I des EU KI- Gesetzes abgedeckt ist und (2) einer Drittbewertung unterzogen werden muss.

   Beispiele: Laut Anhang I betrifft dies KI-gesteuerte Drohnen, die durch die Verordnung 2018/1139 abgedeckt sind, KI-Systeme, die in der Luftsicherheitsausstattung gemäß der Verordnung 300/2008 verwendet werden, sowie KI-gesteuerte drahtlose Geräte, die der Richtlinie 2014/53[5] unterliegen.

2. Und/oder es wird in hochriskanten Sektoren eingesetzt, wie sie in Anhang III des EU-KI-Gesetzes definiert sind.

   Beispiele hierfür sind KI-Systeme, die für folgende Zwecke eingesetzt werden:

   - *für biometrische Identifikation und Emotionserkennung, die nicht in den Bereich verbotener Praktiken fallen. Dazu gehören biometrische Identifikationssysteme, die eine natürliche Person mit zeitlicher Verzögerung (nicht in Echtzeit) und ohne deren aktive Beteiligung durch den Abgleich biometrischer Daten einer Person mit den in einer Referenzdatenbank gespeicherten Daten identifizieren (siehe Seite 16)[6]. Biometrische Verifikations- und Authentifizierungssysteme (z.B. im Rahmen der Zugangskontrolle oder zur Entsperrung eines mobilen Geräts – wie ab Seite 15 beschrieben) sind keine hochriskanten KI-Systeme.*
   - *als Sicherheitskomponenten im Management und Betrieb kritischer Infrastruktur.*
   - *zur Bewertung des Zugangs einer Person zu (beruflicher) Bildung und Ausbildung.*
   - *im Bereich der Beschäftigung und Arbeitnehmerverwaltung, z.B. für Rekrutierungszwecke oder für Entscheidungen zu Arbeitsbedingungen, Aufgabenverteilung, Leistungsbewertung und vertraglichen Beziehungen.*
   - *zur Bewertung und Klassifizierung von Notrufen.*
   - *für Risikoanalysen, z.B. zur Einschätzung von Strafverfolgungsbehörden oder in deren Auftrag, um das Risiko zu bewerten, dass eine natürliche Person Opfer eines Verbrechens wird.*

„Anwender, aber auch Entwickler und Verteiler von hoch-risiko KI-Systemen, müssen ab dem 02. August 2026 den verschiedenen Bestimmungen des EU-KI-Gesetzes entsprechen“

Diese Bestimmungen werden in Kapitel III dieser Charta ab Seite 27 weiter erläutert.

Aber wie kann man sicher wissen, ob ein KI-System Hochrisiko ist oder in einen entsprechend regulierten Anwendungsfall fällt?

Es liegt in der Verantwortung des Anbieters eines KI-Systems, zu bewerten, ob ein KI-System Hochrisiko ist oder nicht und dies zu dokumentieren, bevor das System auf den Markt gebracht oder in Betrieb genommen wird.

Aber es hängt auch vom Anwendungsfall ab. Hochrisiko-Produkte und -Anwendungsfälle sind für Anwender im EU-KI-Gesetz in Artikel 6 sowie in den Anhängen I und III definiert, aber die Verordnung ist komplex.

Die Europäische Kommission wird daher Leitlinien zur Umsetzung der Hochrisiko-Klassifikation entwickeln. In der Zwischenzeit können unsere Querschnittskriterien den Anwendern eine erste Orientierungshilfe bieten.

[5] *Es wird erwartet, dass das EU-KI-Büro weitere Leitlinien zur Wechselwirkung zwischen der Hochrisiko-Definition des EU-KI-Gesetzes und der bestehenden produktbezogenen Gesetzgebung veröffentlicht.*
[6] *Es wird erwartet, dass das EU-KI-Büro weitere Leitlinien zur Definition von KI-Systemen, zu Verboten und zur Klassifizierung von Hochrisiko-KI veröffentlicht.*

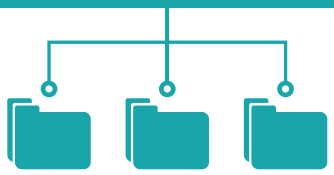
IV. Beispiele für mögliche Niedrigrisiko- und Hochrisiko-KI-Anwendungsfälle

HAFTUNGSAUSSCHLUSS

Dieses Dokument soll Sicherheitsdienstleistungsunternehmen ein erstes Verständnis für mögliche Niedrigrisiko- und Hochrisiko-Systeme und -Anwendungsfälle vermitteln. Die in dieser Charta bereitgestellten Informationen ersetzen nicht system- und anwendungsfallspezifische Risikoanalysen, die vom Anwender durchgeführt werden sollten, um die Einhaltung des EU-KI-Gesetzes sicherzustellen.

Niedrigrisiko

Niedrigrisiko-KI-Anwendungsfälle



Viele KI-Anwendungsfälle in Sicherheitsdienstleistungen können voraussichtlich nicht als Hochrisiko klassifiziert werden. Unter Berücksichtigung des EU-KI-Gesetzes und unserer Querschnittskriterien lassen sich die folgenden Anwendungsfälle in Sicherheitsdienstleistungen eher in die Niedrigrisiko-Kategorie einordnen:

1. Risikomanagement

Durch das Durchsuchen großer Mengen an nicht-personenbezogenen Daten bestehender Sicherheitsinfrastrukturen, wie z. B. Videoüberwachungskameras, können KI-Systeme den Kunden konkrete Informationen über ihre Sicherheitsmaßnahmen und Verbesserungsvorschläge liefern. Beim Einsatz solcher KI-Anwendungen können Sicherheitsdienstleistungsunternehmen schnell konkrete, datengestützte Informationen und vorausschauende Analysen zu Trends und Mustern bereitstellen, wie zum Beispiel:

- Historische Muster von Besucherströmen und Bewegungen
- Spitzenzeiten/Tage/Monate von Besuchern und Straftaten in der Einrichtung oder Umgebung
- Respektive Vulnerabilitätsbewertungen einer Einrichtung basierend auf aktuellen Sicherheitsplänen

Solche Risikoanalysen können fundierte Entscheidungen fördern und Sicherheitsdienste effektiver gestalten. Sicherheitsdienstleistungsunternehmen können Empfehlungen für maßgeschneiderte Lösungen wie Personalbesetzung und den Einsatz spezieller Technologien geben.

2. Analyse der Geschäftsabläufe

KI-Anwendungen können auch die Effizienz interner Geschäftsabläufe analysieren, basierend auf Daten wie:

- Spitzenzeiten der Nutzung bestimmter Geschäftsdienste
- Facility Management, z. B. Energieeffizienz von Gebäuden, Produkten und Fahrzeugflotten
- Besucherverfolgung
- Daten zu Vorfällen im Bereich Arbeitsschutz
- Auswirkungen von erbrachten Dienstleistungen für Marketingzwecke

Die internen Geschäftsabläufe und somit auch die Dienstleistungen, die Kunden angeboten werden, können effizienter, ökologischer und sicherer gestaltet werden. Serviceauswirkungsbewertungen können für Marketingzwecke genutzt werden.

3. Crowd-Management

KI-unterstützte CCTV-Systeme können verwendet werden, um die Anzahl der Menschen bei einer Veranstaltung zu überwachen, automatisch Standorte mit hoher Besucherdichte zu identifizieren, Bewegungsmuster einer Menschenmenge zu analysieren sowie Engpässe zu erkennen, die Sicherheitsrisiken für die Besucher darstellen könnten. Das Personal vor Ort kann dann entsprechende Maßnahmen ergreifen, wie z. B. Zugangskontrollen oder die Steuerung der Menschenmenge.

Diese Systeme sind bei Großveranstaltungen wie Fußballspielen oder Festivals von großem Nutzen und helfen dabei, Ersthelfer und Notfalldienste im Falle eines Vorfalls zu leiten. Der Einsatz solcher Systeme dürfte

jedoch als Hochrisiko-Anwendungsfall eingestuft werden, wenn sie personenbezogene Daten in ihre Analyse und Ausgabe einbeziehen (z. B. wenn sie mit biometrischen Daten arbeiten und diese mit nicht-personenbezogenen Daten kombinieren).

4. Biometrische Verifizierung

Biometrische Verifizierungssysteme unterscheiden sich deutlich von biometrischen Identifikationssystemen:

- Verifizierungssysteme bestätigen, dass eine spezifische Person, die ist, die sie vorgibt zu sein, indem sie biometrische Daten dieser Person mit zuvor bereitgestellten biometrischen Daten vergleichen (Frage: Bist du es?).

- Identifikationssysteme identifizieren eine unbekannte Person ohne deren Zustimmung (Frage: Wer ist es? Siehe Seite 16).

Anhang III des EU-KI-Gesetzes klassifiziert daher biometrische Identifikationssysteme als „Hochrisiko“, nicht jedoch Verifizierungssysteme. Biometrische Verifizierung stellt eine bedeutende Verbesserung der Effizienz und Wirksamkeit der Zugangskontrolle dar, insbesondere bei sensiblen Einrichtungen wie kritischer Infrastruktur.

5. Weitere Anwendungsfälle für KI-unterstützte Analysen nicht-personenbezogener Daten

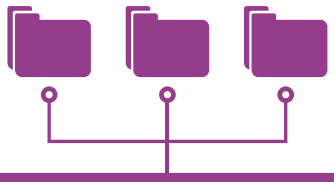
Die Liste möglicher Anwendungsfälle für KI-gestützte Datenanalysen könnte endlos fortgesetzt werden. Besonders im Bereich der Videoüberwachung besteht ein enormes Potenzial, um effizientere, genauere und schnellere Dienstleistungen zu bieten:

- **Alarm-Triage:** KI-unterstützte Kameras können dabei helfen, echte von falschen Alarmen in Alarmempfangsstellen (AES) zu unterscheiden. Zum Beispiel kann eine Kamera anhand von Form- und Bewegungserkennung feststellen, ob ein Rentier das überwachte Gelände betritt oder eine menschliche Person. Das System kann so den Alarm überprüfen, feststellen, ob er möglicherweise falsch ist, und eine entsprechende Empfehlung an den Sicherheitsbeamten im AES weitergeben. Dies kann die Reaktionszeit auf tatsächliche Vorfälle verkürzen und sowohl die Effizienz der Geschäftsabläufe als auch das Schutzniveau für den Kunden verbessern.

- **Objektanalyse:** Ähnlich wie bei der Alarm-Triage können KI-Systeme schnell bestimmte erkannte Objekte analysieren und klassifizieren. Beispielsweise können sie feststellen, ob ein bestimmtes Fahrzeug in einer Sperrzone erlaubt ist (z. B. basierend auf einer Datenbank oder einer weißen Liste „genehmigter“ Kennzeichen). In einem kritischeren Fall kann ein KI-unterstütztes Drohnenerkennungssystem schnell analysieren, ob eine Drohne eine potenziell gefährliche Nutzlast trägt und ihre Geschwindigkeit sowie die voraussichtliche Zeit des Aufpralls bestimmen.

- **Verhaltensdetektion:** CCTV kann durch KI-Anwendungen unterstützt werden, um verdächtige Verhaltensweisen zu identifizieren, die mit Straftaten in Verbindung stehen – z. B. Bewegungspatterns und andere Aktivitäten. KI-Systeme können dann einen entsprechenden Alarm auslösen, der von Sicherheitskräften vor Ort oder in einer AES bewertet wird, bevor präventive Maßnahmen ergriffen werden. Solche Anwendungsfälle verbessern Sicherheitsmaßnahmen und ermöglichen schnelle Reaktionen in kritischen Situationen.

Der Einsatz von KI in Videoüberwachungssystemen kann jedoch schnell in die Kategorie Hochrisiko fallen, abhängig von den verwendeten Daten, dem Grad der menschlichen Aufsicht / Autonomie und der Ausgabe, die das System liefert.



Hochrisiko-KI-Anwendungsfälle

Hochrisiko-KI-Anwendungsfälle können einen erheblichen Nutzen für Sicherheitsdienstleistungsunternehmen bieten, sowohl für Geschäftsabläufe als auch vor allem für die öffentliche Sicherheit insgesamt. Es ist jedoch wichtig, dass ihr Einsatz die Einhaltung des EU-KI-Gesetzes und der in dieser Charta festgelegten Werte garantiert.

Das EU-KI-Gesetz legt viele Produktkategorien und Anwendungsfälle fest, die automatisch als Hochrisikoqualifiziert werden. Basierend auf dieser rechtlichen Definition (siehe Seite 13), die auch mit unseren Querschnittskriterien abgeglichen werden kann, können die folgenden Anwendungsfälle in Sicherheitsdienstleistungen voraussichtlich in die Hochrisiko-Kategorie fallen:

1. Biometrische Identifikation

Das EU-KI-Gesetzidentifiziert Technologien zur biometrischen Identifikation eindeutig als entweder größtenteils verboten (Echtzeit-Identifikation in öffentlichen Räumen) oder als hochrisikobehaftete KI-Systeme (spätere Fernidentifikation). Gesichtserkennungstechnologien sind eine typische Form der biometrischen Identifikation. Zum Zweck der Identifikation vergleichen Gesichtserkennungssysteme eine erfasste Gesichtsabbildung einer natürlichen Person mit einer Datenbank von biometrischen Daten, denen die betroffene Person möglicherweise nicht zugestimmt hat (im Gegensatz zu biometrischen Verifizierung- oder Authentifizierungssystemen, die auf der Zustimmung der betroffenen Person basieren und beispielsweise bei der Zugangskontrolle oder beim Entsperren eines Mobiltelefons verwendet werden).

Der Einsatz biometrischer Identifikationssysteme in öffentlichen Räumen kann einen erheblichen Mehrwert bei der Suche nach Terroristen und anderen relevanten Personen bieten und stellt daher einen großen Nutzen für Strafverfolgungsbehörden und die öffentliche Sicherheit dar. Sie bergen jedoch auch erhebliche Risiken für die Grundrechte der EU-Bürger – insbesondere, weil sie ohne die ausdrückliche Zustimmung der betroffenen Person verwendet werden können.

Betrachtet man unsere übergreifenden Kriterien, bieten diese Systeme autonome Empfehlungen, die in einer „Black Box“ entwickelt werden, basierend auf dem Vergleich mit biometrischen Daten. Der Input basiert auf persönlichen Daten, möglicherweise ohne die Zustimmung der betroffenen Person. Ihre Ziele sind explizit, aber ihre Ergebnisse können rechtliche Konsequenzen für natürliche Personen haben. Dies macht die menschliche Aufsicht über diese Technologie, die all diese Risiken adressiert, besonders wichtig.

Echtzeit-Biometrik-Systeme zur Identifikation sind daher weitgehend durch das EU-KI-Gesetz verboten, während die Verwendung einer zeitverzögerten Identifikation zusätzlichen Schutzvorkehrungen unterliegt, im Vergleich zu anderen Hochrisiko-KI-Systemen[7]. Für weiterführende Hinweise hat die British Security Industry Association (BSIA) einen Leitfaden für die ethische und rechtliche Nutzung von Gesichtserkennungstechnologien veröffentlicht, der unter https://www.bsia.co.uk/ verfügbar ist. Dieser ist besonders nützlich für Sicherheitsdienstleistungsunternehmen, die nicht nur die gesetzliche Einhaltung garantieren, sondern auch wichtige ethische Werte wahren möchten.[8]

2. Emotionserkennung

Emotionserkennungssysteme identifizieren Emotionen oder Absichten einer natürlichen Person basierend auf deren biometrischen Daten. Solche Technologien funktionieren ähnlich wie andere Verhaltensdetektionssysteme, jedoch basiert ihre Nutzung auf der Auswertung von biometrischen Daten einer natürlichen Person, die möglicherweise keine Zustimmung zur Verwendung dieser Daten gegeben hat. Ihr Einsatz kann effizienter sein als bei Niedrigrisiko-KI-gestützten Verhaltensdetektionssystemen. Aber ähnlich wie bei biometrischen Identifikationssystemen erfüllen sie alle übergreifenden Kriterien für hochriskante KI und werden im EU-KI-Gesetz entweder als verboten (z.B. am Arbeitsplatz oder in Bildungseinrichtungen) oder als hochriskante KI-Systeme mit erweiterten Transparenzpflichten klassifiziert.

3. Erkennung verbotener Gegenstände in der Luftsicherheit

Ein typisches Beispiel für KI-gestützte Systeme in der Luftsicherheit sind Automatisierte Systeme zur Erkennung verbotener Gegenstände. Diese Systeme erkennen automatisch verbotene Gegenstände in der

[7] *Zum Beispiel darf keine Entscheidung ausschließlich auf der Grundlage der Ergebnisse dieser Systeme getroffen werden, und die Ergebnisse müssen immer von mindestens zwei ausreichend qualifizierten und autorisierten natürlichen Personen überprüft werden, es sei denn, die Mitgliedstaaten halten diese Anforderung in Strafverfolgungsfällen für unverhältnismäßig.*

[8] *Zusätzlich zum Leitfaden der BSIA wird ein neuer britischer Standard (BS 9347) veröffentlicht, der die Sicherheitsbranche dazu anleitet, sichere und vertrauenswürdige Richtlinien für die Verifizierung und Identifikation entlang der gesamten Lieferkette für Gesichtserkennungstechnologie zu entwickeln.*

Luftsicherheit anhand von Bildern und Daten, die ihnen von den Entwicklern zugeführt wurden. Der Einsatz von KI-unterstützter Luftsicherheitstechnik kann Sicherheitsmaßnahmen und die betriebliche Effizienz an Flughäfen erheblich verbessern – vorausgesetzt, es erfolgt eine angemessene menschliche Aufsicht. KI-gestützte Erkennungssysteme wie die Automatisierten Systeme zur Erkennung verbotener Gegenstände können jedoch auch erhebliche Risiken mit sich bringen, insbesondere aufgrund des Umfelds, in dem sie eingesetzt werden: Das Versäumnis, einen verbotenen Gegenstand im Sicherheitsbereich der Luftfahrt zu erkennen, kann erhebliche Folgen für die öffentliche Sicherheit haben. Das EU-KI-Gesetz stuft sie daher automatisch als hochriskant ein[9], was auch logisch erscheint, wenn wir unsere übergreifenden Kriterien anwenden.

4. KI-unterstützte Drohnen

KI ist heute ein wesentlicher Sicherheitsbestandteil in unbemannten Fahrzeugen – insbesondere bei autonomen Drohnen. KI-Algorithmen ermöglichen es Drohnen, autonom zu fliegen, wodurch der Bedarf an menschlicher Intervention reduziert wird. Drohnen können zudem KI-unterstützte Sensoren und Erkennungssysteme beinhalten, die in Echtzeit Informationen an einen Sicherheitsbeauftragten oder an die autonom fliegende Drohne selbst liefern. KI-gestützte Drohnen können Sicherheitsbeauftragten aus der Ferne dabei helfen, fundierte Entscheidungen in Echtzeit zu treffen. Einsatzkräfte können große Bereiche gleichzeitig mit mehreren Drohnen überwachen, ohne jede einzelne Drohne selbst steuern zu müssen, wodurch Überwachungsaufgaben wesentlich effizienter werden. Darüber hinaus kann die Integration von KI-Systemen die Sicherheit von Drohnenoperationen erhöhen, da sie der Drohne helfen kann, sich an veränderte Flugbedingungen anzupassen, wie z. B. das Betreten von Flugverbotszonen oder sich ändernde Wetterbedingungen. Der erhöhte Grad an Autonomie und die Risiken für die physische Umgebung machen es jedoch notwendig, den Einsatz von KI-unterstützten Drohnen bestimmten Regeln zu unterwerfen. Ein fehlerhaftes autonomes Drohnensystem stellt beispielsweise sowohl für Menschen am Boden als auch für Flugzeuge in der Luft ein Risiko dar. Das EU-KI-Gesetz stuft daher alle KI-Systeme als „hochriskant“ ein, die ein Sicherheitsbestandteil eines Produkts sind oder selbst ein Produkt darstellen, das der EU-Drohnenverordnung unterliegt und eine Drittbewertung durchlaufen muss. [10]

5. HR-Management

Der Einsatz von sogenanntem algorithmischem Management am Arbeitsplatz kann die Aufgabenverteilung und Rekrutierung erheblich unterstützen – besonders in Unternehmen mit einer großen Anzahl von Mitarbeitenden.

- **Aufgabenverteilung:** KI-gestützte Analysen von Geschäftsbetrieb können dem Management Empfehlungen zur Zuteilung von Mitarbeitenden in verschiedenen Diensten und Schichten geben. Es besteht daher ein großes Potenzial, die Arbeitsorganisation zu optimieren, was zu Produktivitätsgewinnen führen kann, die sowohl den Unternehmen als auch den Mitarbeitenden zugutekommen. Gleichzeitig können KI-Systeme die geleistete Arbeit von Mitarbeitenden nicht aus der Perspektive der menschlichen Leistung bewerten, wie es ein menschlicher Manager tun kann, der auch Sozialkompetenzen berücksichtigt. Menschliche Aufsicht ist daher von entscheidender Bedeutung.

- **Rekrutierung:** Wenn sie auf vertrauenswürdigen Daten basieren, kann KI-gestützte Analyse dabei helfen, Stellenprofile besser mit potenziellen Kandidaten abzugleichen – zum Nutzen von Unternehmen, Arbeitssuchenden und integrativen Arbeitsplätzen.

Solche Anwendungsfälle und die damit verbundenen Chancen bringen jedoch auch Risiken mit sich und können Auswirkungen auf die Mitarbeitenden haben – sowohl in Bezug auf die Aufgabenverteilung als auch auf die Chancen auf dem Arbeitsmarkt. Insbesondere bei der Rekrutierung kann KI, je nach Programmierung des Systems, auch zu einer systemischen Diskriminierung bestimmter Arbeitergruppen führen. Die Ausgaben des KI-Systems können zukünftige Karrierechancen, den Lebensunterhalt dieser Personen und die Rechte der Arbeitnehmenden beeinflussen. Der Einsatz von KI im HR-Management wird daher automatisch als hochriskantes KI-System kategorisiert, wenn diese Systeme für die Rekrutierung oder Auswahl von natürlichen Personen oder für Managemententscheidungen zur Beeinflussung der vertraglichen Beziehungen und der Aufgabenverteilung von Mitarbeitenden verwendet werden sollen. Wichtig ist, dass die Betreiber dieser KI-Systeme gemäß dem EU-KI-Gesetz vor dem Einsatz die betroffenen Mitarbeitenden und ihre Vertreter informieren.

---

[9] *Wie alle KI-Systeme, die Teil von Produkten sind, die durch die Verordnung Nr. 300/2008 über gemeinsame Vorschriften im Bereich der Luftsicherheit geregelt sind und die eine Drittbewertung durchlaufen müssen. Es wird erwartet, dass das EU-KI-Büro weitere Leitlinien zur Wechselwirkung zwischen der Definition von hochriskanten KI-Systemen im EU-KI-Gesetz und der bestehenden produktbezogenen Gesetzgebung veröffentlicht.*

[10] *Es wird erwartet, dass das EU-KI-Büro weitere Leitlinien zur Wechselwirkung zwischen der Definition von hochriskanten KI-Systemen im EU-KI-Gesetz und der bestehenden produktbezogenen Gesetzgebung veröffentlicht.*

„Bei der Integration von KI in Dienstleistungen soll sie einen Mehrwert schaffen, indem sie die Komplementarität und Synergie zwischen Menschen und Technologien sicherstellt“

Kapitel II: Chancen und Risiken des Einsatzes von KI in Sicherheitsdienstleistungen

Unsere Beispiele für Anwendungsfälle zeigen, dass der Einsatz von KI viele Vorteile für die öffentliche Sicherheit und die Bürger der Europäischen Union bringen kann. **Die Integration von KI in Sicherheitsdienstleistungen verändert Sicherheitskonzepte, verbessert die betriebliche Resilienz von Unternehmen, macht die Einsätze von Sicherheitskräften sicherer und führt zu effektiveren Sicherheitsdienstleistungen.** Doch während KI-Technologie großes Potenzial bietet Sicherheitsakteuren zu helfen, kriminelle Aktivitäten besser zu erkennen und ihnen entgegenzuwirken, erfordert ihr Einsatz auch sorgfältige Risikobewertungen. Dieses Kapitel beleuchtet die wichtigsten Chancen, die KI-gestützte Dienste für die Bürger, Unternehmen und Arbeiter der Europäischen Union bieten können, aber auch die Hauptfaktoren, die Risiken und unerwünschte Ergebnisse mit sich bringen können.

I. Chancen

1. Höhere Sicherheitsleistung durch Synergie mit menschenzentrierten Dienstleistungen

Die Integration von KI in Sicherheitslösungen ist kein Selbstzweck. Bei der Integration von KI in Dienstleistungen soll sie einen Mehrwert schaffen, indem sie die Komplementarität und Synergie zwischen Menschen und Technologien sicherstellt – den Sicherheitskräften einen „sechsten Sinn“ verleiht und dies in ein bisher unerreichtes Sicherheitsniveau übersetzt.

1.1. Datenbasierte Identifikation, Triage und Minderung von Sicherheitsrisiken in Echtzeit

Neue Fähigkeiten zur Erkennung, Triage und Reaktionszeit auf verdächtige Bewegungen, Eindringlinge oder Anomalien, stellen einen grundlegenden Vorteil der Integration von KI in Sicherheitsdienste dar:

- **Objektanalyse- und verbotene Gegenstände Erkennungssysteme** auf KI-Basis können schnell, erkannte Objekte oder Gefahren analysieren und klassifizieren.
- **Verhaltens- und Emotionserkennungssysteme** (optisch, akustisch) können helfen, ungewöhnliches Verhalten zu identifizieren und die Intervention zu beschleunigen, um den Schutz öffentlicher Räume und kritischer Infrastrukturen zu verbessern.
- **KI-gesteuerte Drohnen- und Anti-Drohnen-Technologie** bieten ein äußerst wertvolles zusätzliches Werkzeug für die Überwachung und Fernbewachung kritischer Infrastrukturen und öffentlicher Räume, insbesondere in großen Bereichen (z.B. Bahngleise, Pipelines, Offshore-Energieinfrastruktur usw.).
- **Fernbiometrische Identifikationssysteme** können einen erheblichen Wert für die gezielte Suche nach

Terroristen, anderen bestimmten Personen von Interesse und gefährdeten Personen bieten.

- **KI** kann helfen, echte von falschen Alarmen in AES zu trennen und die gleichbleibende Qualität des Dienstes aufrechtzuerhalten.

Alle diese Anwendungsfälle bieten nützliche Echtzeitinformationen, die den Sicherheitskräften ein zusätzliches „Gefühl" vermitteln, Sicherheitsmaßnahmen durch verbesserte Entscheidungsfindung optimieren und die Reaktionszeit im Falle eines Vorfalls verkürzen. Sicherheitsdienstleistungen werden damit anspruchsvoller und erreichen ein neues Niveau an „Intelligenz".

1.2. Erhöhte Anpassungsfähigkeit von Sicherheitslösungen

KI macht Sicherheitsdienstleistungen agiler und kann diese in Echtzeit an die Bedürfnisse der Kunden anpassen.

KI-gestützte Risikoanalyse kann fundierte Entscheidungsfindungen vorantreiben und Sicherheitslösungen gezielt auf die spezifischen Bedürfnisse eines Kunden ausrichten. Letztlich stärkt sie die Resilienz einer Einrichtung, verhindert zukünftige Vorfälle durch prädiktive Analysen und erhöht die Sicherheit der Mitarbeitenden und Sicherheitskräfte.

Im **Crowd-Management** kann KI den Sicherheitsdienstleistern schnelle Informationen in herausfordernden Umfeldern und fundierte Entscheidungsfindungen in Echtzeit liefern. Sie macht das Crowd-Management effektiver, ermöglicht schnelle Entscheidungen und Anpassungsfähigkeit von Sicherheits- und Schutzmaßnahmen und verbessert erheblich die Sicherheit bei Veranstaltungen.

1.3. Befähigung der Mitarbeitenden durch Automatisierung

KI unterstützt Sicherheitsmitarbeitende mit neuen Erkenntnissen und Informationen durch die Automatisierung von Aufgaben.

Biometrische Verifikationssysteme helfen Mitarbeitenden, Personen zu authentifizieren und den Zugang zu kontrollieren, insbesondere an sensiblen Einrichtungen wie kritischer Infrastruktur.

Automatisierte Drohnen können den Sicherheitskräften helfen, fundierte Entscheidungen in Echtzeit zu treffen. Sie können große und/oder mehrere Bereiche gleichzeitig überwachen, ohne sie alle steuern zu müssen, was die Überwachungsaufgaben wesentlich effizienter macht. Zudem wird die Sicherheit im Betrieb durch KI-gestützte Berücksichtigung externer Parameter, wie etwa Wetterbedingungen, unterstützt.

Alarm-Triage verhindert, dass Sicherheitskräfte wiederholt störende Fehlalarme validieren müssen (z.B. bei bestimmten Wetterbedingungen wie Schneefall) und hilft ihnen, sich auf ihre Hauptaufgaben zu konzentrieren – so wird eine Informationsüberflutung vermieden. Alle Arten von **KI-gestützten Datenanalysen und optischen/akustischen Sensoren** können die Belastung der Sicherheitskräfte bei Standardaufgaben verringern und die Entscheidungsfindung unterstützen.

1.4. Verbesserter Datenschutz und Cybersicherheit

KI kann den Datenschutz und die Cybersicherheit verbessern, indem sie Analysten bei der beschleunigten Erkennung von Bedrohungen und Anomalien im Datenzugriff unterstützt – und so wertvolle Reaktionszeit spart. KI kann bei der Durchführung von **Cyber-Risikobewertungen** wesentlich unterstützen und helfen, Phishing, Malware und andere böswillige Aktivitäten zu erkennen.

2. Vorteile für Unternehmen und Mitarbeitende

Die Vorteile von KI in Sicherheitsdienstleistungen schließen sich nicht gegenseitig aus: Viele Anwendungsfälle sind nicht nur eine Chance für die öffentliche Sicherheit und den Schutz von Kunden, sondern auch für Sicherheitsdienstleistungsunternehmen und ihre Mitarbeitenden.

2.1. Bessere Sicherheit und Schutz der Mitarbeitenden

Ein zentraler Vorteil des Einsatzes von KI ist ein höheres Schutzniveau für Sicherheitskräfte. KI-gestützte Risikoanalyse kann die beruflichen Gefährdungen von Sicherheitskräften berücksichtigen. KI ermöglicht es den Mitarbeitenden, Risiken zunehmend aus der Ferne zu erkennen und zu validieren. KI-gesteuerte Drohnen und Roboter bieten den Sicherheitskräften nicht nur einen besseren Überblick über potenzielle Risiken, sondern verhindern auch, dass sie gefährliche Umgebungen betreten.

2.2. Förderung integrativer Arbeitsplätze

Die OECD[11] hebt hervor, dass **der Einsatz von algorithmischem Management am Arbeitsplatz dazu beitragen kann, Vielfalt, Inklusion, Gleichberechtigung und Nichtdiskriminierung zu fördern**. Vertrauenswürdige Daten sind dabei entscheidend. Der Einsatz von KI am Arbeitsplatz muss auf relevanten und hochwertigen Daten basieren, um Verzerrungen oder Diskriminierung am Arbeitsplatz zu bekämpfen. Algorithmisches Management kann dann objektivere Bewertungen von Bewerbungen und Leistungsbeurteilungen fördern und bessere Chancen für Anerkennung und Beförderung für Mitarbeitende bieten, die traditionell unter Diskriminierung auf dem Arbeitsmarkt gelitten haben.

2.3. Neue Jobmöglichkeiten

Die verstärkte Befähigung und der verbesserte Schutz der Mitarbeitenden in KI-gestützten Diensten können den Sicherheitsberuf attraktiver machen. In ihrer Forschung hat die OECD herausgefunden, dass in Branchen wie der Fertigung oder dem Finanzwesen die Reduzierung der Zeit, die Mitarbeitende mit wiederholenden Aufgaben verbringen, ihnen eine größere Möglichkeit gibt, Zeit mit strategischen Aufgaben[12] zu verbringen. Darüber hinaus können Aufgaben im Zusammenhang mit KI-gestützten Diensten neue Mitarbeitergruppen ansprechen, die derzeit in den europäischen Sicherheitsdiensten unterrepräsentiert sind, zum Beispiel Frauen und junge Menschen.

2.4. Optimierung von Geschäftsprozessen und Wettbewerbsfähigkeit

Die datengetriebene Optimierung von Geschäftsprozessen kann die operative Resilienz stärken, zur Aufrechterhaltung der Servicequalität beitragen und intelligentere Investitionen ermöglichen – was die Wettbewerbsfähigkeit in der Branche steigert. KI kann betriebliche Prozesse kosteneffizienter, umweltfreundlicher und sicherer gestalten, was Vorteile für Arbeitnehmer, Sicherheitsdienstleistungsunternehmen und Kunden bietet, z.B. durch eine bessere Einsatzplanung von Personal oder die Optimierung von Patrouillenrouten.

II. Risiken

Neben den Chancen ist es wichtig zu erkennen, dass der Einsatz von KI auch mit Risiken verbunden sein kann. Ein ausgewogenes Verhältnis zwischen der Nutzung des Potenzials von KI und der Minderung ihrer Risiken erfordert eine sorgfältige Betrachtung der ethischen, rechtlichen, gesellschaftlichen und sicherheitsrelevanten Implikationen des jeweiligen Einsatzes.

Dieses Kapitel bietet einen kurzen Überblick über wichtige Risikokategorien, die mit dem Einsatz von KI in Sicherheitsdienstleistungen verbunden sind.

[11] *OECD (2023), OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market, OECD Publishing, Paris, https://doi.org/10.1787/08785bba-en.*
[12] *OECD (2023), OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market, OECD Publishing, Paris, https://doi.org/10.1787/08785bba-en.*

Risikofaktoren

Wenn wir über Risiken im Zusammenhang mit dem Einsatz von KI sprechen, konzentriert sich der öffentliche Diskurs oft auf die möglichen negativen Auswirkungen ihrer Nutzung. Wir sollten jedoch zunächst die Risikofaktoren betrachten. Für die Anwender gibt es fünf Hauptfaktoren, die sich gegenseitig verstärken und vor sowie während des Einsatzes von KI ganzheitlich adressiert werden sollten:

1. Mangel an sorgfältigen Risikomanagementprozessen

KI ist keine beliebige Technologie. Das Fehlen eines sorgfältigen, spezifischen Risikomanagementprozesses während des Lebenszyklus der Nutzung eines KI-Systems kann zu einer Nichteinhaltung relevanter Gesetze (wie z. B. des EU-KI-Gesetzes oder der DSGVO) und unerwarteten Risiken für die Gesundheit, Sicherheit oder die Grundrechte von Bürgern und Sicherheitsmitarbeitern führen.

2. Verwendung von unzuverlässigen und voreingenommenen Datensätzen

Die Nutzung von unzuverlässigen Daten bei KI-Einsätzen kann zu verstärkten Verzerrungen in den KI-Entscheidungen, unzuverlässigen Ergebnissen und Risiken für die Grundrechte führen. Sie untergräbt die Erklärbarkeit, Verantwortlichkeit und das Vertrauen in KI-Systeme, was potenziell zu erheblichen Reputationsrisiken für die Anwender führen kann.

3. Mangel an menschlicher Aufsicht

Die menschliche Aufsicht ist von zentraler Bedeutung für den Einsatz von KI in Sicherheitsdienstleistungen. Fehlt sie, kann dies eine Folge von Personalmangel oder von Personal sein, das nicht ausreichend geschult oder geführt wird, um das System im jeweiligen Anwendungsfall effektiv zu betreiben. Eine unzureichende menschliche Aufsicht kann dazu führen, dass die Funktionsweise und der Output des KI-Systems nicht mehr erklärt werden kann. Das Personal kann sich zu sehr auf die Ergebnisse des Systems verlassen, z.B. durch falsch positive oder negative Ergebnisse. Ein Mangel an menschlicher Aufsicht schränkt nicht nur die menschliche Autonomie ein, leitet sie fehl und/oder untergräbt sie, sondern ist auch ein wesentlicher Faktor für die Gefährdung der Gesundheit, der Sicherheit und der Grundrechte der Bürger.

4. Mangel an Resilienz

KI-Systeme und ihre Algorithmen müssen gegenüber physischer Manipulation und Cyberangriffen resilient sein. Andernfalls können ihre Funktionsweise und Ergebnisse beeinflusst oder sogar lahmgelegt werden – was insbesondere in Sicherheitsdienstleistungen zu erheblichen Risiken führen kann.

5. Mangel an KI-Management

Eine dedizierte KI-Management-Politik sollte einen Verantwortlichen benennen und eine klare Prozess- und Verantwortungsstruktur festlegen – wobei die endgültige Verantwortung und Haftung für den richtigen oder missbräuchlichen Einsatz von KI beim Vorstand oder dem Leitungsgremium des Anwenders liegen sollte. Ohne eine solche Politik besteht die Gefahr, dass die rechtlich Verantwortlichen sich auf die „glaubhafte Abstreitbarkeit" berufen und dass die Führungsebene des Unternehmens, das die KI einsetzt, ohne Beteiligung des Vorstands gehandelt hat.

Risikokategorien

Diese Risikofaktoren können sich in vielfältige, anwendungsspezifische materielle und immaterielle Risiken übersetzen. Wir fassen sie hier in verschiedenen Kategorien zusammen.

1. Risiken für die Grundrechte der Bürger

In der öffentlichen Debatte über die allgemeine Nutzung von KI werden Ängste geäußert, dass Grundrechte aufgrund von:

- einem Verlust der menschlichen Autonomie und der Erklärbarkeit von KI-Systemen
- Misstrauen gegenüber verschiedenen Anwendungsfällen und deren beabsichtigten Zwecken / Zielen
- Bedenken bezüglich des Datenschutzes und der Datensätze, die als Eingabedaten für das KI-System verwendet werden
- Verletzungen wichtiger Grundrechte durch die Ausgaben des Systems nicht gewahrt werden könnten.

Verletzungen der Grundrechte können materiell oder immateriell sein, einschließlich physischer, psychologischer, gesellschaftlicher oder wirtschaftlicher Schäden. Risiken, die mit dem Einsatz von KI zu Strafverfolgungszwecken verbunden sind, beinhalten häufig Ängste vor Massenüberwachung und invasiver Überwachung, Verstößen gegen den Datenschutz, diskriminierenden Sicherheitspraktiken und der Verantwortlichkeit im Falle eines Systemausfalls und der damit verbundenen Folgen[13]. Schutzmaßnahmen gegen diese Risiken werden im EU-KI-Gesetz behandelt und sind entscheidend für den ethischen und rechtlichen Einsatz von KI in den Sicherheitsdienstleistungen (siehe Kapitel III).

[13] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html

2. Risiken für die Rechte der Arbeitnehmer sowie für den Arbeits- und Gesundheitsschutz

Der Einsatz von KI kann auch Risiken für Arbeitnehmer mit sich bringen. Dies betrifft insbesondere Risiken im Zusammenhang mit algorithmischen Werkzeugen zur Mitarbeiterführung[14][15] und umfasst:

- Diskriminierung von Arbeitnehmern durch die Verwendung voreingenommener Datensätze bei der Einführung algorithmischer Personalverwaltungssysteme während der Rekrutierungsprozesse, Vertragsverlängerungen, Aufgabenverteilung und Zugang zu Schulungen.
- Wahrnehmung einer hochstressigen Arbeitsumgebung, die mit einem intensiveren Arbeitstempo, erhöhter Komplexität der Aufgaben und Informationsflüsse sowie dem Gefühl ständiger Überwachung, Beobachtung und Bewertung verbunden ist.
- Reduzierung der menschlichen Interaktion mit Kollegen und Vorgesetzten, wenn von den Arbeitnehmern erwartet wird, dass sie zunehmend isoliert arbeiten.

Das EU-KI-Gesetz und andere europäische Gesetzgebungen setzen Schutzmaßnahmen gegen diese Risiken um.

3. Reputationsrisiken für Unternehmen

Vertrauen ist entscheidend für die Arbeit von Sicherheitsdienstleistungsunternehmen und für den Einsatz von KI. Die EU hat 2019 ethische Leitlinien für den vertrauenswürdigen Einsatz von KI veröffentlicht, in denen betont wird, dass jeder Einsatz rechtlich einwandfrei, ethisch und robust sein muss, um Vertrauen aufzubauen.[16] Daten aus dem Jahr 2023 bestätigen jedoch, dass das öffentliche Vertrauen in die Technologie noch immer gering ist.[17]

In Europa war das öffentliche und mediale Interesse an KI in den letzten Jahren hoch, auch aufgrund mehrerer Vorfälle (siehe Seite 23). Häufig fällt der Fokus auf Organisationen, die Fehler machen. Wenn ein Unternehmen keine Transparenz über den Einsatz von KI zeigt, unzureichend qualifiziertes Personal für die KI-Überwachung einsetzt und Risiken schlecht managt, was zu Zwischenfällen führt, kann es schnell als unethisch und rücksichtslos gegenüber Arbeitnehmenden, Kundinnen und Kunden sowie Bürgerinnen und Bürgern wahrgenommen werden. Wie bei jeder neuen Technologie kann ein einzelner Vorfall dazu genutzt werden, das potenzielle Risiko zu verallgemeinern und die weitere Entwicklung zu gefährden oder zu verlangsamen.

4. Sicherheitsrisiken

Der Einsatz von KI in Sicherheitsdienstleistungen birgt von Natur aus Sicherheitsrisiken, insbesondere wenn Risikofaktoren nicht angemessen adressiert werden. Unzureichende menschliche Aufsicht sowie ein Mangel an physischer und cybertechnischer Resilienz des Systems können zu wichtigen Fehlfunktionen des Systems führen, die Auswirkungen auf die öffentliche Sicherheit haben:

- Unzureichend qualifizierte Mitarbeitende könnten sich von falschen Negativmeldungen mit wichtigen Folgen nicht bewusst sein, z.B. in der Flughafensicherheit.
- Böswillige Akteure könnten ein KI-System sowohl physisch als auch durch Cyberangriffe manipulieren, um eine Fehlfunktion des Systems auszulösen und kriminelle Handlungen vorzubereiten.[18]
- Ungenauigkeit und Vorurteile in Trainingsmodellen sowie die Komplexität von Systemen können zu falschen Aussagen und Ergebnissen des KI-Systems (so genannte „Halluzinationen“[19]) führen, was zu unerwünschten Folgen führt und das Vertrauen in das System untergräbt.[20]
- KI bietet böswilligen Akteuren neue Werkzeuge und kann für Deepfakes[21] und Cyberangriffe[22] genutzt werden. Sie könnten darüber hinaus Daten im KI-System hacken, wie z.B. biometrische Daten, um sozial manipulierte Cyberangriffe durchzuführen und Sicherheitsprotokolle zu umgehen.

5. Sekundäreffekte

Der Einsatz von KI-Systemen kann Sekundäreffekte haben, die vor ihrem Einsatz leicht übersehen werden können, wenn keine geeigneten Risikomanagement-Verfahren vorhanden sind. Ein Beispiel: Der Einsatz von intelligenten GPS-Systemen kann den Verkehrsfluss in einer Stadt erheblich verbessern, könnte jedoch auch zu einer vermehrten und unerwünschten Nutzung von Nebenstraßen in Wohngebieten führen. Das gleiche gilt für datengestützte Sicherheitsrisikoanalysen. Während diese den Schutz und die Sicherheit eines bestimmten Objekts erheblich verbessern können, könnte dies auch Auswirkungen auf Mietpreise und Versicherungspolicen in bestimmten Stadtteilen haben.

---

[14] *Baiocco, S., Fernández-Macías, E., Rani, U. and Pesole, A., The Algorithmic Management of work and its implications in different contexts, Seville: European Commission, 2022, JRC129749*

[15] *OECD (2023), OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market, OECD Publishing, Paris, https://doi.org/10.1787/08785bba-en.*

[16] *https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai*

[17] *https://kpmg.com/xx/en/home/insights/2023/09/trust-in-artificial-intelligence.html#:~:text=AI%20trust%20and%20acceptance,depend%20on%20the%20AI%20application.&text=Three%20in%20five%20(61%20percent,wary%20about%20trusting%20AI%20systems.&text=67%20percent%20report%20low%20to%20moderate%20acceptance%20of%20AI.*

[18] *https://csrc.nist.gov/pubs/ai/100/2/e2023/final*

[19] *KI-Halluzinationen bezeichnen eine Situation, in der ein KI-System unsinnige, bizarre und ungenaue Ausgaben erzeugt. Dies kann aufgrund unvollständiger Systemmodellierung, komplexer Interaktionen in Deep-Learning-Systemen oder wenn das System Muster oder Objekte wahrnimmt, die entweder nicht existieren oder für den Menschen nicht wahrnehmbar sind, auftreten.*

[20] *https://www.economist.com/science-and-technology/2024/02/28/ai-models-make-stuff-up-how-can-hallucinations-be-controlled*

[21] *https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf*

[22] *https://www.wired.com/story/here-come-the-ai-worms/*

WIE WIR AUS VERGANGENEN VORFÄLLEN UND BESTEHENDEN RISIKEN LERNEN KÖNNEN

Clearview AI

Im Jahr 2020 berichtete die New York Times[23], dass Clearview AI, ein US-amerikanisches Unternehmen für Gesichtserkennungssoftware, mehr als 3 Milliarden Gesichtsabbildungen aus sozialen Medien gesammelt hatte, einschließlich zusätzlicher Daten wie Namen von Personen, und diese in einer Datenbank speicherte. Der Zugriff auf diese Datenbank wurde an Strafverfolgungsbehörden verkauft, so dass diese, eine Person sofort anhand eines Fotos identifizieren konnten. Die Datenschutzbehörden meldeten erhebliche ethische und datenschutzbezogene Bedenken gegen dieses Geschäftsmodell an, und die Datenschutzbehörden in Frankreich und Deutschland wiesen das Unternehmen an,, seine Geschäftstätigkeiten einzustellen und alle personenbezogenen Daten zu löschen.[24]

Skandal um Kindergeldzahlungen in den Niederlanden

Von 2013 bis 2019 setzten die niederländischen Steuerbehörden einen selbstlernenden Algorithmus ein, um Risikoprofile zur Aufdeckung von Kindergeldbetrug zu erstellen. Auf Basis der Empfehlungen des Systems wurden Familien bereits bei bloßem Verdacht auf Betrug bestraft. Infolgedessen fielen zehntausende Familien, oft aus einkommensschwachen Schichten oder ethnischen Minderheiten in Armut, da sie hohe Schulden gegenüber der Steuerbehörde hatten. Die niederländische Datenschutzbehörde (DPA) stellte mehrere Verstöße gegen die EU-Datenschutzvorschriften fest und verhängte eine Geldstrafe von 3,7 Millionen Euro gegen die Steuerbehörde.[25]

Physische Eingriffe oder Cyberangriffe, die das Verhalten von KI-Systemen manipulieren

Wissenschaftler des US-amerikanischen National Institute for Standards and Technology warnen, dass KI-Systeme versagen können, wenn ein Angreifer einen physischen oder cyberbasierten Weg findet, um deren Entscheidungsfindung zu manipulieren.[26] Autonome Fahrzeuge lernen aus Straßenbildern, wo und wie sie fahren müssen, während Chatbots Gesprächsprotokolle analysieren, um Antworten vorherzusagen. Allerdings können Trainingsdaten durch korrupte Daten verfälscht werden. Hacker könnten einen Cyberangriff auf KI-Systeme durchführen, um auf sensible Informationen zuzugreifen und diese zu missbrauchen. Der Input in das System könnte physisch verändert werden, um das System zu verwirren oder zu manipulieren.

Der Skandal der britischen Post

Das IT-System der britischen Post, Horizon, beschuldigte zwischen 2000 und 2014 fälschlicherweise Hunderte von Postangestellten finanzieller Unregelmäßigkeiten, die nicht durch menschliches Versagen, sondern durch Fehler in der IT-Software verursacht wurden. Über 900 Mitarbeiter wurden wegen Diebstahls, Betrugs und falscher Buchführung angeklagt – was dazu führte, dass unschuldige Personen mit falschen Anschuldigungen und strafrechtlichen Verfolgungen konfrontiert wurden. Zahlreiche Postbeamte hatten Probleme mit der Software dem Management gemeldet, und selbst der Softwareanbieter war sich der Fehler bewusst. Dennoch wurden die Bedenken von der britischen Post nicht gehört. Auch wenn die Horizon-Software kein KI-System war, zeigt dieser Vorfall die Bedeutung der menschlichen Aufsicht, Datenqualität und Systemalgorithmen, KI-Management-Politiken und Risikomanagementprozesse.

[23] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
[24] https://www.law.kuleuven.be/citip/blog/clearview-ai-illegally-collecting-and-selling-our-faces-in-total-impunity-part-ii/
[25] https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/#:~:text=In%202019%20it%20was%20revealed,on%20the%20system's%20risk%20indicators.
[26] https://csrc.nist.gov/pubs/ai/100/2/e2023/final

WAS WIR DARAUS LERNEN KÖNNEN

Diese Beispiele zeigen, wie schnell der Einsatz von KI in konkrete Risiken umschlagen kann. Es ist daher wichtig, Risikotreiber von Anfang an ganzheitlich anzugehen:

1. **Risikomanagementprozesse während des gesamten Lebenszyklus eines KI-Systems** sind entscheidend, um fallbezogene Risiken zu identifizieren und anzugehen sowie die Einhaltung von Vorschriften sicherzustellen. Für den Einsatz von Gesichtserkennungssystemen veröffentlichte die BSIA einen hilfreichen „Leitfaden für den ethischen und rechtlichen Einsatz von automatisierter Gesichtserkennung".[27]

2. Der Einsatz **von KI-Systemen, die auf vertrauenswürdigen Daten und Algorithmen basieren**, ist entscheidend für vertrauenswürdige Ausgaben und die Vermeidung von Verletzungen der Grundrechte.

3. **Qualitative menschliche Aufsicht mit ausreichend qualifiziertem Personal** ist entscheidend, um sicherzustellen, dass stets eine Person die Empfehlung des KI-Systems bewerten und eine endgültige, unabhängige Entscheidung treffen kann.

4. **Hohe Sicherheitsstandards und Cyber-Resilienz während des gesamten Lebenszyklus des KI-Systems** sind entscheidend, um Bürger, Nutzer und Kunden vor Fehlfunktionen eines KI-Systems zu schützen.

5. **Klare Berichtslinien, Prozesse und Verantwortlichkeiten** als Teil der KI-Management-Politik sind entscheidend, damit Betreiber im Falle einer Fehlfunktion oder eines Missbrauchs eines KI-Systems geeignete Maßnahmen ergreifen können.

„Vertrauen ist entscheidend für die Arbeit von Sicherheitsdienstleistungsunternehmen und für den Einsatz von KI"

[27] https://www.bsia.co.uk/zappfiles/bsia-front/public-guides/form_347_automated_facial%20recognition_a_guide_to_ethical_and_legal_use-compressed.pdf

Kapitel III: Werte und Anforderungen

CoESS' MISSION

Unsere Mission ist es, das Wachstum in der Sicherheitsdienstleistungsbranche durch die Förderung hochwertiger Lösungen und Professionalität zu unterstützen, basierend auf der Auswahl und Entwicklung qualifizierter Mitarbeiter und Technologien. Dieses Ziel wird durch die Förderung qualitativ hochwertiger Schulungen und Arbeitsbedingungen der Mitarbeiter, die Einhaltung von Vorschriften und Industriestandards, höchste Sicherheitsstandards für Mitarbeitende, Kundinnen und Kunden sowie Bürgerinnen und Bürger und das Vertrauen von Personen und Behörden in die Branche erreicht.

CoESS fördert die Integration von KI-Systemen in Sicherheitsdienstleistungen im Rahmen ihrer Mission. Bei der Integration von KI geht es nicht nur darum, Technologie in Sicherheitskonzepte zu integrieren, sondern sicherzustellen, dass Menschen und Technologie einander ergänzen und optimieren, um neue Qualitäts- und Effizienzlevels in den Sicherheitsdienstleistungen zu erreichen.

Der Einsatz von KI-Lösungen sollte dem Prinzip der technologischen Neutralität folgen, mit dem Ziel, die beste und zuverlässigste Sicherheitsdienstleistung zu erbringen, sei es durch Menschen oder durch die Kombination mit KI.

Die Einführung von KI sollte einem wertorientierten Verhaltenskodex folgen. In diesem Kapitel werden diese Werte definiert und ein Überblick über die wichtigsten Anforderungen gegeben, um den Anbietern von KI im Sicherheitsbereich zu helfen, diese zu erfüllen – basierend auf dem EU-KI-Gesetz, den OECD-Prinzipien für KI[28] und den EU-Ethischen Leitlinien für vertrauenswürdige KI.[29]

I. CoESS' übergreifende Werte für den ethischen und verantwortungsvollen Einsatz von KI

Die CoESS definiert die folgenden acht übergreifende, miteinander verbundenen Werte für den ethischen und verantwortungsvollen Einsatz von KI in den Sicherheitsdienstleistungen:

1. Respekt der Grundrechte: Die europäische Sicherheitsdienstleistungsindustrie soll eine führende Rolle im ethischen und verantwortungsvollen Einsatz von KI übernehmen. Anbieter von KI-Systemen müssen jederzeit die vollständige Achtung der Charta der Grundrechte der Europäischen Union sicherstellen.[30]

2. Förderung von Vielfalt, Gleichheit, Inklusion und Nichtdiskriminierung: Der Einsatz von KI durch Sicherheitsdienstleister soll Vielfalt, Gleichheit, Inklusion und Nichtdiskriminierung vorantreiben.[31]

3. Menschenzentrierte KI: Der Einsatz von KI-Systemen muss stets von ausreichend geschultem Personal überwacht werden, entsprechend dem jeweiligen Anwendungsfall. Der Einsatz von KI-Systemen in Sicherheitsdienstleistungen soll die Mitarbeitenden

[28] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[29] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[30] *Die Charta (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT) umreißt die in der EU geschützten Grundrechte. Sie umfasst bürgerliche, politische, wirtschaftliche und soziale Rechte, einschließlich des Rechts auf Unversehrtheit der Person, des Rechts auf Freiheit und Sicherheit, des Schutzes personenbezogener Daten, des Rechts auf Achtung des Privatlebens sowie der Freiheit der Bewegung, der Meinungsäußerung und der Informationsfreiheit. Die Charta verbietet Diskriminierung aus verschiedenen Gründen wie Rasse, Geschlecht, Religion und sexueller Orientierung. Sie garantiert Rechte wie faire Arbeitsbedingungen, das Recht der Arbeitnehmer auf Information, das Recht auf Tarifverhandlungen und kollektives Handeln, das Recht auf gute Verwaltung und hohe Verbraucherschutzstandards*

[31] *Im Einklang mit der EU-Charta der Grundrechte (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT) und der Erklärung der sektoralen Sozialpartner der EU zu Vielfalt, Gleichstellung, Inklusion und Nichtdiskriminierung im Bereich der privaten Sicherheitsdienste CoESS und UNI Europa (2024)*

befähigen, informierte Entscheidungen auf der Grundlage neuer Erkenntnisse und Informationen zu treffen. Menschenzentrierte KI bedeutet auch besseren Schutz für Menschen, indem deren Grundrechte und Prinzipien im Hinblick auf Nichtdiskriminierung, Transparenz und Datenschutz gefördert werden. Für die CoESS bedeutet der menschenzentrierte Einsatz von KI auch, dass KI ein öffentliches Gut wird und den europäischen Bürgern in allen Bereichen dient.

4. Transparenz und Erklärbarkeit: Der Einsatz von KI muss für die beteiligten Interessengruppen transparent sein, entsprechend dem jeweiligen Anwendungsfall. Die Erklärbarkeit der Funktionsweise und der Ausgaben von KI-Systemen ist entscheidend, nicht nur für den ethischen und verantwortungsvollen Einsatz von KI, sondern auch für das öffentliche Verständnis und Vertrauen.

5. Datenschutz: Die Datenverwaltung entlang der Wertschöpfungskette des Einsatzes muss die Datenschutzrechte der europäischen Bürger sicherstellen, die in der Charta der Grundrechte der EU und der DSGVO verankert sind.

6. Physische und cyber-resiliente Sicherheit: KI-Systeme und deren Einsatz in Sicherheitsdienstleistungen müssen sicher, resilient und robust sein, um Zwischenfälle zu verhindern, ihnen standzuhalten und sie zu überwinden. Systeme müssen auf eine wiederholbare und vorhersehbare Weise arbeiten, und ein konsistentes Qualitätsniveau der Dienstleistungen muss während des gesamten Einsatzes des KI-Systems gewährleistet sein. Unbeabsichtigte materielle und immaterielle Schäden an Mitarbeitenden und betroffenen Interessengruppen müssen minimiert und verhindert werden.

7. Rechenschaftspflicht: Die gesamte Wertschöpfungskette der Entwicklung und des Einsatzes von KI-Systemen muss entsprechend ihren Rollen und rechtlichen Anforderungen für die ordnungsgemäße Funktionsweise der KI-Systeme verantwortlich sein.

8. Nachhaltigkeit: Der Einsatz von KI muss ganzheitlich zur Erreichung der nachhaltigen Entwicklungsziele der Vereinten Nationen beitragen, indem er inklusives Wachstum, (ökologisch) nachhaltige Entwicklung und Wohlstand fördert. Es muss sichergestellt werden, dass KI-Lösungen nachhaltig und umweltfreundlich sind – unter Berücksichtigung der Auswirkungen der Betriebe auf die Umwelt.

„Der Einsatz von KI sollte einem wertebasierten Verhaltenskodex folgen“

II. Erste Schritte, um einen ethischen und verantwortungsbewussten Einsatz von KI sicherzustellen

Der Kernzweck dieser Charta besteht darin, den Anwendern von KI-Systemen in Sicherheitsdienstleistungen, Leitlinien für die rechtlichen und freiwilligen Anforderungen für den ethischen und verantwortungsvollen Einsatz von KI bereitzustellen, die auf die in Kapitel II identifizierten Risiken eingehen, basierend auf den übergreifenden Werten der CoESS. Bevor der Einsatz eines KI-Systems beschlossen und geeignete Maßnahmen getroffen werden, um dessen verantwortungsvollen und ethischen Einsatz zu garantieren, sollten die Anwender drei vorbereitende Schritte im Rahmen eines Multi-Stakeholder-Ansatzes unternehmen[32]:

Schritt 1: Identifizierung des KI-Systems

Als ersten Schritt sollte der Anwender feststellen, ob er tatsächlich ein KI-System einsetzen möchte, bevor er es kauft. Obwohl KI-Systeme von den Anbietern als solche gekennzeichnet werden sollten, ist dies nicht immer der Fall, insbesondere bei Systemen, die vor der Umsetzung des EU-KI-Gesetzes vermarktet wurden. Der Anwender sollte daher mit dem Anbieter und/oder intern die zugrunde liegende Technologie des Systems für den jeweiligen Anwendungsfall überprüfen. Nach der „KI-Definition“ im EU-KI-Gesetz (siehe Seite 8) qualifiziert sich ein System als KI, wenn es maschinelles Lernen oder Deep Learning-Modelle verwendet, um Ausgaben wie Vorhersagen, Inhalte, Empfehlungen und Entscheidungen auf der Grundlage von Dateneingaben zu erzeugen. Eine Überprüfung der übergreifenden Kriterien (siehe Seite 10) kann dabei helfen.

Schritt 2: Bewertung der geltenden rechtlichen Regelungen und Beurteilung, ob das KI-System und der Anwendungsfall gemäß dem EU-KI-Gesetz als niedrig- oder hochriskant einzustufen sind

Vor jeder Nutzung sollte der Anwender den Zweck und das beabsichtigte Ergebnis des Einsatzes des KI-Systems definieren und eine Bewertung vornehmen, um zu verstehen, ob das KI-System und der Anwendungsfall als niedrig- oder hochriskant einzustufen sind. Diese Bewertung ist entscheidend, um das EU-KI-Gesetz

[32] *Die CoESS empfiehlt, diese Anforderungen in einem Multi-Stakeholder-Ansatz zu bewerten und umzusetzen, wobei unter anderem die verantwortlichen Projektmanager, Manager für regulatorische Angelegenheiten und Compliance-Experten, technische KI-Experten, Datenschutzbeauftragte, Personalabteilungen, Sicherheitsfachleute sowohl im Bereich der physischen Sicherheit als auch der Cybersicherheit sowie Geschäftsbereichsleiter des betreffenden Servicesegments einbezogen werden sollten. Solche Teams sollten vielfältig sein, um potenzielle Verzerrungen während des Betriebs eines KI-Systems zu erkennen. KI-Richtlinien und Verhaltenskodizes müssen eine Priorität auf Vorstandsebene im Unternehmen haben.*

einzuhalten und KI verantwortungsvoll und ethisch zu nutzen. Die Bewertung sollte mit den folgenden Fragen beginnen:

1. **Ist das KI-System oder der Anwendungsfall gemäß dem EU-KI-Gesetz verboten (siehe Seite 12)?**

2. **Qualifiziert sich mein Unternehmen nur als Anwender oder auch als Anbieter des KI-Systems?** Wenn der Anwender seinen Namen auf das KI-System setzt oder Änderungen am System oder seiner beabsichtigten Nutzung vornimmt, wird er gemäß dem EU-KI-Gesetz als Anbieter eines KI-Systems[33] betrachtet, was zusätzliche gesetzliche Verpflichtungen im Fall von hochriskanten KI-Systemen nach sich zieht.

3. **Qualifiziert sich das KI-System oder der Anwendungsfall als hochriskant?** Unsere übergreifenden Kriterien können bei einer ersten Bewertung helfen. Um rechtliche Sicherheit zu erlangen, sollte der Anwender folgendes prüfen:

   a. Ob das betreffende KI-System mit dem CE-Kennzeichen versehen und in einer offiziellen, öffentlich zugänglichen EU-Datenbank registriert ist (verfügbar bis zum 2. August 2026).

   b. Ob der Anwendungsfall in eine der hochriskanten Kategorien fällt, die im Anhang III des EU-KI-Gesetzes definiert sind (siehe Seite 13).

4. **Werden in einem Anwendungsfall verschiedene KI-Systeme kombiniert** (z.B. Installation von Crowd-Management-Systemen auf einem KI-unterstützten Drohnensystem) und wenn ja, wie wirkt sich dies auf die Kategorisierung des Anwendungsfalls als niedrig- oder hochriskant aus?

5. Wenn das KI-System oder der Anwendungsfall nicht als hochriskant eingestuft wird, **interagiert das System im Anwendungsfall mit natürlichen Personen** und birgt daher Transparenzrisiken (siehe Seite 12)?

Schritt 3: Bewertung des Mehrwerts des Einsatzes des KI-Systems

Vor der Nutzung des KI-Systems sollte der Anwender bewerten, ob die Integration von KI im spezifischen Anwendungsfall einen Mehrwert bietet und welchen spezifischen Zweck und welches Ergebnis der Einsatz verfolgen soll. Anschließend sollte der Anwender potenzielle Vorteile, Nachteile und unbeabsichtigte Auswirkungen der Integration von KI in den betreffenden Service bewerten, und diese gegen das übergeordnete Ziel der Verbesserung der Qualität und Effektivität abwägen. Diese Bewertung sollte Faktoren wie die Wirksamkeit im Einsatz, die Auswirkungen auf die Arbeitsbedingungen und die Entscheidungsfindung, die Qualifikation der Mitarbeiter und den Bedarf an Weiterqualifizierung sowie die Kosteneffizienz berücksichtigen.

III. Anforderungen für den ethischen und verantwortungsvollen Einsatz von KI

HAFTUNGSAUSSCHLUSS

Dieses Dokument soll Sicherheitsdienstleistungsunternehmen ein erstes Verständnis des EU-KI-Gesetzes und wichtiger Verhaltenskodizes vor und während der Nutzung eines KI-Systems vermitteln. Die in dieser Charta bereitgestellten Informationen ersetzen keine system- und anwendungsspezifischen Risiko- und Regulierungsbewertungen, die vom Betreiber durchgeführt werden sollten, um die Einhaltung des EU-KI-Gesetzes sicherzustellen.

KI-Akteure sind für das ordnungsgemäße Funktionieren von KI-Systemen verantwortlich, basierend auf ihren Rollen, dem Kontext und im Einklang mit dem Stand der Technik. Um die Einhaltung unseres Wertsystems, des EU-KI-Gesetzes und anderer relevanter Gesetzgebungen sicherzustellen, empfiehlt diese Charta den Betreibern, eine KI-Management-Politik zu entwickeln, die die rechtliche Verantwortung und Rechenschaftspflicht für den guten oder missbräuchlichen Einsatz von KI dem Vorstand oder dem leitenden Gremium des Betreibers zuweist. Darüber hinaus soll der Betreiber in einem Multi-Stakeholder-Ansatz[34] einen internen Verhaltenskodex entwickeln, der folgende Maßnahmen umfasst:

[33] *Wenn der Betreiber seinen Namen oder seine Marke auf ein KI-System setzt, dieses erheblich verändert oder den vorgesehenen Zweck des KI-Systems (im Vergleich zu den Anweisungen des Anbieters) ändert, kann der Betreiber gemäß Artikel 25 des EU-KI-Gesetzes zudem als Anbieter eines hochriskanten KI-Systems eingestuft werden und muss daher eine weitaus größere Anzahl an rechtlichen Verpflichtungen erfüllen, die in dieser Charta dargelegt sind.*

[34] *Die CoESS empfiehlt, diese Anforderungen in einem Multi-Stakeholder-Ansatz zu bewerten und umzusetzen, einschließlich (unter anderem) der verantwortlichen Projektmanager, Manager für regulatorische Angelegenheiten und Compliance-Experten, technische KI-Experten, Datenschutzbeauftragte, Personalabteilung, Sicherheitsfachleute sowohl im Bereich der physischen als auch der Cyber-Sicherheit sowie der Geschäftsbereichsleiter des betroffenen Service-Segments. Solche Teams sollten vielfältig sein, um auch potenzielle Verzerrungen (Bias) während des Betriebs eines KI-Systems zu erkennen. KI-Politiken und Verhaltenskodizes müssen eine Priorität des Unternehmensvorstands sein.*

1 RISIKOMANAGEMENT

Risikomanagementsysteme sind gemäß Artikel 9 des EU-KI-Gesetzes eine gesetzliche Verpflichtung für hochriskante KI-Systeme

Die mit der Einführung eines KI-Systems verbundenen Risiken müssen über den gesamten Lebenszyklus des Systems hinweg und entsprechend dem beabsichtigten Zweck sowie dem Kontext der Nutzung angemessen gemanagt werden. Zu diesem Zweck soll der Betreiber ein Risikomanagementsystem einrichten, um:

- die Einhaltung der relevanten Gesetze sicherzustellen, einschließlich der DSGVO und des EU-KI-Gesetzes
- bekannte, vernünftigerweise vorhersehbare und andere mögliche Risiken zu identifizieren und zu analysieren, die das KI-System für die Gesundheit, Sicherheit oder die Grundrechte von EU-Bürgern und -Arbeitnehmern sowie die Sicherheit der Kunden darstellen könnte, wenn es gemäß dem vorgesehenen Zweck eingesetzt wird, aber auch unter Bedingungen von vernünftig vorhersehbarem Missbrauch
- geeignete und gezielte, technisch und physisch machbare Risikomanagementmaßnahmen zu ergreifen, um die identifizierten Risiken auf ein vernünftigerweise akzeptables Niveau zu minimieren
- Notfallverfahren und andere geeignete Milderungs- und Kontrollmaßnahmen einzuführen, die Risiken adressieren, die nicht vollständig beseitigt werden können.

Diese Maßnahmen müssen alle in dieser Charta aufgeführten Anforderungen berücksichtigen und die in Kapitel II identifizierten Risikotreiber und Risikokategorien angemessen adressieren. Es existieren viele internationale Normen[35] und Leitlinien[36], die Betreibern bei der Durchführung von Risikomanagementprozessen helfen können.

2 DATEN-MANAGEMENT

Daten-Management ist eine gesetzliche Verpflichtung für hochriskante KI-Systeme gemäß des EU-KI-Gesetzes, Art. 10 & 26

Die Betreiber müssen sorgfältige Praktiken im Umgang mit Daten sicherstellen:

- Das Daten-Management muss die vollständige Übereinstimmung mit der DSGVO garantieren.
- Es muss eine angemessene cyber- und physische Sicherheit der Datensätze, einschließlich personenbezogener und sensibler Daten, gewährleistet sein – einschließlich der relevanten Rechenzentren.
- Der Einsatz von KI in Sicherheitsdienstleistungen muss auf vertrauenswürdigen, robusten und qualitativ hochwertigen Daten basieren. Zu diesem Zweck müssen die Sorgfaltspflichtverfahren bei der Auswahl von KI-Systemen sicherstellen, dass die Anbieter das KI-System mit Eingabedaten trainiert, validiert und getestet haben, die bestimmten Qualitätskriterien entsprechen und potenzielle Verzerrungen ausschließen, gemäß des – EU-KI-Gesetzes. Soweit der Betreiber Kontrolle über die Eingabedaten ausübt, muss er sicherstellen, dass diese in Bezug auf den beabsichtigten Zweck des hochriskanten KI-Systems relevant sind.

Das Daten-Management muss zudem die Nachvollziehbarkeit der Datenverarbeitung, die Erklärbarkeit der Ausgaben des KI-Systems sowie die Auditierbarkeit und Rechenschaftspflicht gewährleisten.

3 MENSCHLICHE AUFSICHT

Viele Maßnahmen zur menschlichen Aufsicht sind eine gesetzliche Verpflichtung für Betreiber von hochriskanten KI-Systemen gemäß des EU-KI-Gesetzes, Art. 4, 14 und 26

Eine angemessene menschliche Aufsicht über jedes KI-System ist zentral für die Erfüllung der in dieser Charta festgelegten Werte. Das EU-KI-Gesetz sieht daher zu Recht in ihrem Artikel 4 vor, dass Betreiber von KI-Systemen bereits ab dem 02. Februar 2025 Maßnahmen ergreifen müssen, um das KI-Wissen ihrer Mitarbeiter nach besten Kräften sicherzustellen. Für die europäischen Sicherheitsdienstleistungsunternehmen unterstreicht die CoESS, dass verantwortliche Mitarbeiter befähigt werden müssen, die Anforderungen dieser Charta zu erfüllen,

[35] *Wie zum Beispiel ISO/IEC 23894 „Künstliche Intelligenz – Leitlinien für das Risikomanagement" und ISO/IEC 42001 „Managementsystem für Künstliche Intelligenz".*

[36] *Dazu gehören die EU-Selbsteinschätzungsliste für vertrauenswürdige KI (https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment), das UK-Portfolio von KI-Absicherungstechniken, einschließlich des Anekanta AI Risk Intelligence Systems (https://www.gov.uk/ai-assurance-techniques) für biometrische und hochriskante KI, sowie das AI Risk Management Framework (https://www.nist.gov/itl/ai-risk-management-framework) des US National Institute of Standards and Technology.*

angemessen und verhältnismäßig zum spezifischen Anwendungsfall.

Die Betreiber müssen geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass sie KI-Systeme gemäß den beiliegenden Gebrauchsanweisungen der Systeme verwenden.

Der Betreiber muss weiter sicherstellen, dass die Mitarbeiter, die KI-Systeme überwachen, durch angemessene Schulungen, Qualifikationen, technische und operationelle Maßnahmen, einschließlich der Delegation von Befugnissen, befähigt werden:

- Die Gebrauchsanweisungen, den beabsichtigten Zweck und den Anwendungsfall des KI-Systems sowie die Schlussfolgerungen aus dem Risikomanagement zu verstehen
- Die relevanten Fähigkeiten und Einschränkungen des KI-Systems zu verstehen
- Sich des Genauigkeitsgrads, der Robustheit und der Cybersicherheit des KI-Systems bewusst zu sein – einschließlich aller bekannten und vorhersehbaren Umstände, die Auswirkungen auf die Genauigkeit, Robustheit und Cybersicherheit haben könnten
- Sich der Bedingungen für vernünftigerweise vorhersehbare Fehlanwendungen bewusst zu sein, die zu Risiken für die Gesundheit, Sicherheit oder die Grundrechte der betroffenen Personen aufgrund der Ausgaben des Systems führen könnten
- Die betroffenen Personen über den beabsichtigten Zweck der Datensammlung aufzuklären und Informationen darüber bereitzustellen, wie die Ausgaben des KI-Systems zustande gekommen sind
- Sich über Änderungen des KI-Systems bewusst zu sein, die seine Leistung beeinträchtigen könnten[37]
- Dass der Betrieb des KI-Systems ordnungsgemäß zu überwachen ist, einschließlich der Erkennung und Verwaltung von Anomalien, Funktionsstörungen und unerwarteter Ergebnisse
- Sich der möglichen Auswirkungen bewusst zu bleiben, sich automatisch oder übermäßig auf die Ausgaben eines KI-Systems zu verlassen
- Die Ausgaben des hochriskanten KI-Systems korrekt zu interpretieren und autonome Entscheidungen zu treffen
- In jeder bestimmten Situation zu entscheiden, das KI-System nicht zu verwenden oder seine Ausgaben anderweitig zu ignorieren, zu überschreiben oder rückgängig zu machen
- In den Betrieb des KI-Systems einzugreifen und relevante Notfallverfahren sowie andere geeignete Minderung und Kontrollmaßnahmen im Falle eines Vorfalls zu ergreifen
- Den Anbieter und relevante öffentliche Stellen im Falle eines Vorfalls zu informieren.

Im Fall von hochriskanten KI-Einsätzen verlangt Artikel 14 des EU-KI-Gesetzes sorgfältige Richtlinien und Prozesse des Betreibers, um die gesetzliche Konformität sicherzustellen. Besondere Aufsichtsregelungen bestehen für Anwendungen der biometrischen Identifikation.[38]

Betreiber müssen dringend die potenzielle Notwendigkeit zur Weiterbildung der Mitarbeiter vor der Einführung von KI berücksichtigen. Die private Sicherheitsbranche sollte eng mit den öffentlichen Behörden zusammenarbeiten, um die Integration von KI-Systemen in die Dienstleistungen vorzubereiten und, falls erforderlich, Schulungsrahmenwerke anzupassen, die Anforderungen für KI-Kompetenz, Fähigkeiten, Qualifikationen und Lizenzanforderungen widerspiegeln. Der soziale Dialog kann eine wichtige Rolle spielen, um diesen Prozess zu leiten und den verantwortungsvollen Einsatz von KI am Arbeitsplatz im Interesse der beruflichen Gesundheit, Sicherheit und Arbeitsqualität zu gewährleisten.

„Der soziale Dialog kann eine wichtige Rolle bei der Förderung eines verantwortungsvollen Einsatzes von KI am Arbeitsplatz spielen“

[37] *Personen, die in menschlicher Aufsicht geschult sind, können auch das Risiko verringern, dass unvoreingenommene KI-Systeme während ihrer Nutzung voreingenommene Entscheidungen treffen. Je nach Anwendungsfall sollten Mitarbeiter geschult werden, die KI-Implementierung während des gesamten Betriebs an menschenzentrierten Werten auszurichten.*

[38] *Im Fall von Anwendungsfällen zur biometrischen Identifizierung schreibt Artikel 14.5 des EU-KI-Gesetzes vor, dass keine Maßnahme oder Entscheidung auf der Grundlage der Ausgabe des Systems getroffen wird, es sei denn, diese wurde zuvor von mindestens zwei natürlichen Personen mit der erforderlichen Kompetenz, Ausbildung und Befugnis separat überprüft und bestätigt. Ausnahmen von dieser Regelung bestehen für Anwendungsfälle, die der Strafverfolgung dienen.*

4 RESILIENZ

Maßnahmen zur Genauigkeit, Robustheit und Cybersicherheit von KI-Systemen sind eine gesetzliche Verpflichtung für Betreiber von hochriskanten KI-Systemen gemäß EU-KI-Gesetzes, Art. 15

Im Einklang mit dem EU-KI-Gesetz und anderen relevanten Gesetzen, wie dem EU-Rechtsakt zur Cyberresilienz, hat der KI-Systemanbieter die Verantwortung, seine Produkte so zu entwerfen und zu entwickeln, dass deren Genauigkeit, Resilienz und Cybersicherheit angemessen gewährleistet werden.

Die Betreiber müssen jedoch auch die erforderlichen technischen, operativen und organisatorischen Maßnahmen ergreifen, um auf relevante physische und Cybersicherheitsrisiken zu reagieren, im Einklang mit einer vorhergehenden Risikobewertung, dem beabsichtigten Zweck und der Anwendungsumgebung. KI-Systeme müssen robust, sicher und zuverlässig während ihres gesamten Lebenszyklus sein, sodass sie unter normalen Nutzungsbedingungen, bei vorhersehbarer Nutzung oder Missbrauch oder unter anderen widrigen Umständen angemessen, wiederholbar und vorhersehbar funktionieren und kein unzumutbares Sicherheitsrisiko darstellen. Es ist daher wichtig, dass physische und Cyber-Risiken ganzheitlich adressiert werden.[39]

- Die physische Manipulation von KI-Systemen kann zu fehlerhaften Ausgaben und damit zu erheblichen Sicherheitsrisiken führen. Physische Schutzmaßnahmen können Zugangskontrollen und Überwachungen von physischen KI-Hardware-, Infrastruktur- und Datenspeicherkomponenten umfassen; die Aufrechterhaltung optimaler Umweltbedingungen für das Funktionieren der KI-Systeme; und die Implementierung sicherer Verfahren für die Entsorgung von KI-Systemen. Mitarbeiter sollten ordnungsgemäß geschult werden, um diese Maßnahmen umzusetzen. Ein besonderer Fokus sollte auch auf die Sicherheit und Resilienz von Rechenzentren gelegt werden.
- Cyberangriffe auf das KI-System während des Betriebs können die Trainingsdaten oder Modelle „vergiften“ oder erhebliche Datenschutz- und Sicherheitsrisiken darstellen. Es gibt Standards[40] und Richtlinien[41] im Bereich der Cyber-Resilienz, die für die Betreiber von KI-Systemen nützlich sein können.

Besonders im Bereich von Sicherheitsdienstleistungen ist eine beispielhafte physische- und Cyber-Resilienz des KI-Systems entscheidend, um Zwischenfälle zu vermeiden und den Ruf des Betreibers nicht zu gefährden. Um Zwischenfälle zu bewältigen und die Geschäftskontinuität zu gewährleisten, sollten Betreiber Notfallverfahren und Krisenpläne einrichten. Sicherheitsbeauftragte müssen möglicherweise den Betrieb des KI-Systems im jeweiligen Anwendungsfall übernehmen. Daten können an geografisch verteilten Standorten gespeichert werden, um die Auswirkungen lokalisierter physischer Störungen und Cyberangriffe zu minimieren.

5 DOKUMENTATION

Dokumentation ist eine gesetzliche Verpflichtung für hochriskante KI gemäß EU-KI-Gesetz, Art. 12 & 26

Automatische Dokumentation ist gemäß dem EU-KI-Gesetz ein obligatorisches technisches Merkmal für hochriskante KI-Systeme und Betreiber, soweit es unter deren Kontrolle steht. Es ist wichtig, dass Betreiber den Respekt gegenüber Werten im Hinblick auf Nachvollziehbarkeit, Erklärbarkeit und Verantwortlichkeit sicherstellen. Im Verhältnis zum beabsichtigten Zweck des Systems gewährleistet die Dokumentation der operativen Leistung von KI-Systemen, dass der Betreiber nachverfolgen, erklären und rechtfertigen kann, wie Entscheidungen getroffen werden. Verantwortung erfordert klare Aufzeichnungen, um festzulegen, wer für den Betrieb von KI-Systemen (und mögliche Änderungen daran) verantwortlich ist, und dabei Transparenz und (freiwillige) Einhaltung regulatorischer Anforderungen zu gewährleisten. Das EU-KI-Gesetz sieht eine Aufbewahrungsfrist von mindestens sechs Monaten vor, wenn hochriskante KI-Systeme eingesetzt werden, und legt zusätzliche Verpflichtungen fest, wenn Fernbiometrie-Systeme eingesetzt werden.

---

[39] *Weitere Informationen finden Sie im White Paper der CoESS und der International Security Ligue zum Thema „Cyber-Physische Sicherheit und Kritische Infrastruktur“, verfügbar unter www.coess.eu.*

[40] *Der ISO-Standard „ISO/IEC CD 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems“ behandelt die Cybersicherheitsrisiken von KI-Systemen.*

[41] *Ebenso die „Leitprinzipien zur Behebung der Cybersicherheitsanforderungen für hochriskante KI-Systeme“ (https://op.europa.eu/en/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-en) des Gemeinsamen Forschungszentrums der EU. Die CoESS und Euralarm haben allgemeinere Cybersecurity-Richtlinien für die Sicherheitsbranche veröffentlicht, verfügbar unter: https://www.coess.eu/.*

6 TRANSPARENZ UND ERKLÄRBARKEIT

Verschiedene Transparenzmaßnahmen sind eine gesetzliche Verpflichtung für hochriskante und begrenzt riskante KI-Systeme gemäß dem EU-KI-Gesetz, Art. 13, 26, 49, 50 und 71

Die Einhaltung der DSGVO ist ein zentraler Aspekt des ethischen und verantwortungsvollen Einsatzes von KI. Aber es geht noch weiter: Betreiber von KI-Systemen sollten sich zu Transparenz, Erklärbarkeit und verantwortungsvoller Offenlegung im Hinblick auf KI-Systeme verpflichten.

- **Transparenz gegenüber den betroffenen Personen**: Menschen müssen immer wissen, dass sie mit einem KI-System interagieren und/oder dessen Ergebnissen unterliegen, und dies auf eine rechtmäßige Weise, die im Verhältnis zum jeweiligen Anwendungsfall steht. Die Informationen zur Transparenz sollten aussagekräftig, kontextbezogen, dem Stand der Technik entsprechend und für Menschen mit Behinderungen zugänglich sein. Betroffene Personen müssen in die Lage versetzt werden, die Ergebnisse und damit verbundene Entscheidungen zu verstehen und, wenn nötig, herauszufordern. Arbeitnehmervertreter müssen über den Einsatz von KI-Systemen in der Arbeitnehmerverwaltung informiert werden. Je nach Anwendungsfall und KI-System sollte der Betreiber transparente und zugängliche Beschwerdemechanismen einrichten, die spezifische Rechte und Abhilfemaßnahmen für Einzelpersonen respektieren, die unrechtmäßig von KI-Systemen betroffen sind.

- **Transparenz gegenüber der breiten Öffentlichkeit**: Wenn hochriskante KI-Systeme im Auftrag öffentlicher Behörden eingesetzt werden, muss der Betreiber diese gemäß Art. 49 und 71 des EU-KI-Gesetzes in einer öffentlich zugänglichen europäischen Datenbank[42] registrieren. Um die Transparenz und das Vertrauen der Öffentlichkeit in den Einsatz von KI in Sicherheitsdienstleistungen zu erhöhen und, falls dies im jeweiligen Anwendungsfall als angemessen und sicher angesehen wird, können Betreiber auch freiwillig alle hochriskanten KI-Einsätze registrieren, auch wenn sie diese nicht im Auftrag einer öffentlichen Behörde durchführen.

- **Transparenz gegenüber Behörden**: Betreiber sollten die Dokumentation von KI-Systemen den zuständigen Behörden zur Inspektion zur Verfügung stellen, um die Einhaltung der rechtlichen Anforderungen sicherzustellen. Betreiber von Fernbiometrie-Systemen müssen jährlich Berichte an die relevanten Marktaufsichts- und Datenschutzbehörden einreichen.

- **Erklärbarkeit**: Es ist ferner wichtig, dass Betreiber in der Lage sind, den beabsichtigten Zweck der Datenerhebung den betroffenen Personen zu erklären und klare sowie einfache Informationen darüber bereitzustellen, wie die Entscheidungen des KI-Systems im Verhältnis zum Anwendungsfall und unter Berücksichtigung von geistigem Eigentum, Datenschutz und Sicherheit zustande kamen. Zu diesem Zweck sollten Betreiber, falls erforderlich, den Entwickler auffordern, Modellkarten oder anderweitig für den Menschen lesbare Anleitungen bereitzustellen, die erklären, wie das KI-System Entscheidungen trifft.

Betreiber sollten zudem das Verständnis der Öffentlichkeit und der politischen Entscheidungsträger für den Einsatz von KI in Sicherheitsdienstleistungen fördern. Dies kann durch die Förderung dieser Charta erreicht werden.

7 GRUNDRECHTSFOLGENABSCHÄTZUNG

Bewertungen der Auswirkungen auf die Grundrechte sind eine gesetzliche Verpflichtung für Betreiber von Hochrisiko-KI-Systemen gemäß Artikel 27 des EU-KI-Gesetzes

Zusätzlich zur gesetzlich vorgeschriebenen Datenschutzfolgenabschätzung gemäß der DSGVO, Artikel 25, müssen Betreiber von Hochrisiko-KI, die öffentliche Behörden sind oder Dienstleistungen im Auftrag öffentlicher Behörden erbringen, eine Bewertung der Auswirkungen auf die Grundrechte gemäß Artikel 27 des EU-KI-Gesetzes durchführen, bevor sie ein Hochrisiko-KI-System erstmals einsetzen. Eine solche Bewertung muss Folgendes abdecken:

- eine Beschreibung der Prozesse des Betreibers, in denen das Hochrisiko-KI-System gemäß dem vorgesehenen Zweck eingesetzt wird

- eine Beschreibung des Zeitraums, während dem und der Häufigkeit, mit der das Hochrisiko-KI-System voraussichtlich verwendet wird

- die Kategorien von Personen, die voraussichtlich von der Nutzung des Systems im spezifischen Kontext betroffen sein werden

- die spezifischen Risiken von Schäden, die die betroffenen Personen wahrscheinlich erleiden werden

- eine Beschreibung der Maßnahmen zur menschlichen Aufsicht gemäß den Gebrauchsanweisungen

- Risikomanagementmaßnahmen, einschließlich internem Management und Beschwerdemechanismen.

[42] *Diese EU-Datenbank wird gemäß Artikel 71 des EU-KI-Gesetzes geregelt. Die Informationen, die von den Betreibern von KI-Systemen eingetragen werden müssen, sind in Anhang VIII aufgeführt. Die Datenbank wird von der Europäischen Kommission eingerichtet und verwaltet.*

Betreiber von Hochrisiko-KI-Systemen, die Dienstleistungen im Auftrag öffentlicher Behörden erbringen, müssen ihre nationalen Behörden über diese Bewertung informieren und die Bewertung wiederholen, wenn sie der Ansicht sind, dass eines dieser Elemente während der Nutzung nicht mehr aktuell ist. Betreiber, die keine Hochrisiko-KI-Systeme im Auftrag öffentlicher Behörden einsetzen, sollten ebenfalls eine solche Bewertung in Betracht ziehen, wenn sie Grund zur Annahme haben, dass ihr Anwendungsfall mit unwahrscheinlichen, aber möglichen Auswirkungen auf die Grundrechte verbunden sein könnte. Das EU-KI-Büro könnte Leitlinien entwickeln, die den Betreibern helfen, ihren rechtlichen Verpflichtungen nachzukommen.

Je nach Anwendungsfall können Betreiber betroffene Interessengruppen in die Bewertung der Auswirkungen auf die Grundrechte einbeziehen.

8 SORGFALTSPFLICHT

Betreiber von KI-Systemen sollten Sorgfaltspflichtrichtlinien beim Kauf von KI-Systemen beachten:

- Überprüfen, dass das KI-System auf qualitativ hochwertigen, vielfältigen und repräsentativen Datensätzen trainiert wurde.
- Bestätigen, dass das KI-System den wichtigen Cybersicherheitsanforderungen entspricht, mindestens denen, die im relevanten Gesetz wie dem EU-KI-Gesetz und dem EU-Rechtsakt zur Cyberresilienz festgelegt sind.
- Nur KI-Systeme verwenden, die in ihren Entscheidungsprozessen transparent sind und angemessene Gebrauchsanweisungen[43] enthalten, die unter anderem ein leichtes Verständnis des vorgesehenen Zwecks des Systems und der erforderlichen menschlichen Aufsicht ermöglichen; den Grad der Genauigkeit, einschließlich der Metriken, der Robustheit und der Cybersicherheit; sowie vorhersehbare Umstände und Missbräuche, die zu Risiken für die Grundrechte führen können.

Anbieter von Hochrisiko-KI-Systemen müssen ihre Produkte in der EU-Datenbank gemäß Artikel 71 des EU-KI-Gesetzes registrieren. Betreiber dürfen nur Hochrisiko-Systeme verwenden, die ordnungsgemäß registriert sind.

9 EINBEZIEHUNG DER ARBEITNEHMER IN DIE INTEGRATION VON KI IN DIENSTLEISTUNGEN

Zusätzlich zu den gesetzlichen Verpflichtungen, die Arbeitnehmer über den Einsatz von KI am Arbeitsplatz zu informieren[44], sollte der Betreiber, Sicherheitsbeauftragte aktiv in die Einführung von KI-Systemen in den Dienstleistungen einbeziehen.

Dies könnte Sensibilisierungsmaßnahmen umfassen, wie z. B. Seminare, Webcasts und anderes Informationsmaterial, um Transparenz darüber zu schaffen, welche KI-Systeme verwendet werden und warum und wie sie eingesetzt werden sollen. Als Teil der Maßnahmen zur menschlichen Aufsicht und angepasst an den jeweiligen Anwendungsfall müssen die Arbeitnehmer ein angemessenes Verständnis darüber erhalten, was vom System erwartet werden kann und was nicht, um eine Überforderung der Arbeitnehmer zu vermeiden und Selbstgefälligkeit zu verhindern. Die Vorteile der KI-Risikoanalyse sollten alle Mitarbeiter erreichen, z.B. durch die Weitergabe von Statistiken und Empfehlungen zu Gesundheit und Sicherheit am Arbeitsplatz.

Betreiber können spezielle Anlaufstellen einrichten, bei denen Arbeitnehmer ethische Bedenken hinsichtlich der Funktionsweise und Nutzung bestimmter KI-Systeme vorbringen können, die gemäß dem relevanten Arbeitsrecht geschützt sind, möglicherweise auch über einen Ethik- oder internen Prüfungsausschuss.

10 IM ZWEIFELSFALL: KONTAKT MIT DEN ZUSTÄNDIGEN BEHÖRDEN AUFNEHMEN

Interne Verhaltenskodizes und KI-Richtlinien sollten vorsehen, dass Betreiber aktiv mit den zuständigen Behörden zusammenarbeiten, wenn Zweifel an der rechtlichen Sicherheit und den in dieser Charta festgelegten Anforderungen bestehen. Wenn der Betreiber außerdem Grund zur Annahme hat, dass der Einsatz der KI-Systeme ein materielles oder immaterielles Risiko für betroffene Personen darstellen könnte, sollte er die Systemanbieter und die zuständige Marktüberwachungsbehörde informieren und den Einsatz des Systems aussetzen. Im Falle eines Vorfalls mit einem Hochrisiko-KI-System müssen die zuständigen Behörden informiert werden.

„Diese Charta empfiehlt den Betreibern, eine KI-Governance-Strategie festzulegen“

[43] Für hochriskante KI-Systeme, die den Bestimmungen des EU-KI-Gesetzes in Artikel 13 entsprechen.
[44] gemäß Artikel 26.7 des EU-KI-Gesetzes.

Kapitel IV: Checkliste

Das EU-KI-Gesetz wird ab dem 02. August 2026 schrittweise in Kraft treten. Vieles bei der Umsetzung und der Einhaltung des EU-KI-Gesetzes hängt jedoch von den Leitlinien ab, die vom EU-KI-Büro der Europäischen Kommission veröffentlicht werden, sowie von den Standards, die von CEN/CENELEC entwickelt werden, und dem Durchsetzungsrahmen, der von den nationalen Behörden festgelegt wird.

Wenn Sie bereits KI-Systeme in Ihren Dienstleistungen einsetzen oder dies planen, gibt es Möglichkeiten, der Entwicklung voraus zu sein und mit dieser Charta, Management-Rahmen für KI zu schaffen, die eine ethische und verantwortungsvolle Nutzung von KI in Ihren Dienstleistungen garantieren.

Hier ist eine Checkliste, die Ihnen helfen kann:

- **#1** Richten Sie ein internes Management- und Führungsteam für KI ein und definieren Sie Prozesse und Verantwortlichkeiten, in einem Multi-Stakeholder-Ansatz. ☑
- **#2** Identifizieren Sie die relevanten KI-Systeme sowie deren beabsichtigte Nutzung und Zweck in Ihrem Dienstleistungsangebot. ☑
- **#3** Machen Sie sich mit den rechtlichen Rahmenbedingungen und Standards vertraut, die für Ihren Anwendungsfall gelten, und bestätigen Sie die Fristen zur Einhaltung. ☑
- **#4** Bewerten Sie das mögliche Risikoprofil Ihres KI-Systems und Anwendungsfalls, die jeweiligen rechtlichen Verpflichtungen und den Mehrwert des Einsatzes des KI-Systems im spezifischen Anwendungsfall. ☑
- **#5** Nehmen Sie Kontakt zu Ihren nationalen Behörden und/oder rechtlichen Experten auf und bestätigen Sie Ihre interne Bewertung. ☑
- **#6** Lassen Sie sich von dieser Charta inspirieren und erstellen Sie einen internen Verhaltenskodex. ☑
- **#7** Kaufen Sie Ihr KI-System unter Berücksichtigung Ihrer Sorgfaltspflichten ein und qualifizieren Sie Ihr KI-Führungsteam weiter. ☑
- **#8** Führen Sie eine Risikobewertung durch und setzen Sie einen Risikomanagementprozess für jeden einzelnen Anwendungsfall um. ☑
- **#9** Bereiten Sie geeignete Maßnahmen für jeden einzelnen Anwendungsfall gemäß den in dieser Charta festgelegten Werten und Anforderungen vor und qualifizieren Sie Ihre Belegschaft, wenn nötig, entsprechend weiter. ☑
- **#10** Überprüfen Sie kontinuierlich Ihre KI-Management, überwachen Sie das regulatorische Umfeld und Vorfälle mit Hochrisiko-KI und arbeiten Sie mit dem EU-KI-Büro, den Regulierungsbehörden in Ihrem Land, Normierungseinrichtungen, Branchenverbänden und der KI-Community zusammen, um über die neuesten Trends, Leitlinien, Standards und rechtlichen Entwicklungen informiert zu bleiben. ☑

Sammlung nützlicher Leitlinien und Standards

→ **Rechtstext des EU-KI-Gesetzes:**
https://eur-lex.europa.eu/eli/reg/2024/1689/oj

→ **EU-Leitlinien:**

- Folgen Sie dem EU-KI-Büro:
  https://digital-strategy.ec.europa.eu/en/policies/ai-office
- Folgen Sie dem EU-KI-Pakt:
  https://digital-strategy.ec.europa.eu/en/policies/ai-pact
- Folgen Sie der Europäischen KI-Allianz:
  https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance
- EU-Leitlinien für vertrauenswürdige KI:
  https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- Gemeinsames Forschungszentrum der EU "Leitprinzipien zur Adressierung der Cybersicherheitsanforderungen für Hochrisiko-KI-Systeme":
  https://op.europa.eu/en/publication-detail/-/publication/7d0a4007-51dd-11ee-9220-01aa75ed71a1/language-en
- EU-Selbstbewertungs-Liste für vertrauenswürdige KI:
  https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

→ **Internationale Leitlinien:**

- OECD-Definition eines KI-Systems:
  https://oecd.ai/en/wonk/ai-system-definition-update
- Internationale Vereinigung der Datenschutzprofis (IAPP) – KI-Ressourcenzentrum:
  https://iapp.org/
- Portfolio der KI-Absicherungstechniken des Vereinigten Königreichs:
  https://www.gov.uk/ai-assurance-techniques
- Rahmenwerk des US National Institute of Standards and Technology (NIST) für KI-Risikomanagement:
  https://www.nist.gov/itl/ai-risk-management-framework

→ **Leitlinien der Sicherheitsbranche:**

- British Security Industry Association (BSIA): Automatisierte Gesichtserkennung – Ein Leitfaden für ethische und rechtliche Nutzung:
  https://www.bsia.co.uk/
- CoESS & Euralarm Cybersicherheitsrichtlinien für die Sicherheitsindustrie:
  https://www.coess.eu

→ **Europäische Standards:**
Folgen Sie dem CEN-CENELEC Gemeinsamen Technischen Komitee 21 “Künstliche Intelligenz”:
https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/

→ **Internationale Standards:**

- ISO/IEC 5339:2024 “Informationstechnologie – Künstliche Intelligenz – Leitlinien für KI-Anwendungen”:
  https://www.iso.org/standard/81120.html
- ISO/IEC TS 8200:2024 “Informationstechnologie – Künstliche Intelligenz – Kontrollierbarkeit von automatisierten KI-Systemen”:
  https://www.iso.org/standard/83012.html
- ISO/IEC 22989:2022 “Informationstechnologie – Künstliche Intelligenz – Konzepte und Terminologie der Künstlichen Intelligenz”:
  https://www.iso.org/standard/74296.html
- ISO/IEC 23894 “Künstliche Intelligenz – Leitlinien zum Risikomanagement”:
  https://www.iso.org/standard/77304.html
- ISO/IEC TR 24028:2020 “Informationstechnologie – Künstliche Intelligenz – Überblick über die Vertrauenswürdigkeit in Künstliche Intelligenz”:
  https://www.iso.org/standard/77608.html
- ISO/IEC TR 24030:2024 “Informationstechnologie – Künstliche Intelligenz – Anwendungsfälle”:
  https://www.iso.org/standard/84144.html
- ISO/IEC TR 24368:2022 “Informationstechnologie – Künstliche Intelligenz – Überblick über ethische und gesellschaftliche Bedenken”:
  https://www.iso.org/standard/78507.html
- ISO/IEC TR 27563:2023 “Sicherheit und Datenschutz in Künstliche Intelligenz Anwendungsfällen – Beste Praktiken”:
  https://www.iso.org/standard/80396.html
- ISO 30434:2023 “Humanressourcenmanagement – Personalzuweisung”:
  https://www.iso.org/standard/68711.html
- ISO/IEC 38507:2022 “Informationstechnologie – IT-Governance – Governance-Auswirkungen der Nutzung von Künstlicher Intelligenz durch Organisationen”:
  https://www.iso.org/standard/56641.html
- ISO/IEC 42001 “Künstliches Intelligenz-Managementsystem”:
  https://www.iso.org/standard/81230.html

Acting as the voice of the **security industry**

Confederation of European Security Services

Private security services in Europe provide a wide range of essential services, both for **private** and **public clients**, ranging from **Critical Infrastructure facilities** to **public spaces** and **supply chains**.

coess.eu

Confederation of European Security Services
Avenue des Arts 56
B-1000 Brussels
Belgium