



EUROPÄISCHE
KOMMISSION

Brüssel, den 22.5.2023
C(2023) 3215 final

ANNEXES 1 to 2

ANHÄNGE

des

DURCHFÜHRUNGSBESCHLUSSES DER KOMMISSION

**über einen Normungsauftrag an das Europäische Komitee für Normung und das
Europäische Komitee für elektrotechnische Normung zur Unterstützung der
Unionspolitik im Bereich der künstlichen Intelligenz**

ANHANG I

Liste der zu erarbeitenden neuen europäischen Normen und europäischen Normungsunterlagen

Referenzangaben	
1.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zu Risikomanagementsystemen für KI-Systeme
2.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zur Governance und Qualität von Datensätzen, die zur Entwicklung von KI-Systemen verwendet werden
3.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zur Aufzeichnung durch Protokollierungsfunktionen von KI-Systemen
4.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zur Transparenz und Information der Nutzer von KI-Systemen
5.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zur menschlichen Aufsicht über KI-Systeme
6.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zu Spezifikationen für die Genauigkeit von KI-Systemen
7.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zu Spezifikationen für die Robustheit von KI-Systemen
8.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zu Spezifikationen für die Cybersicherheit von KI-Systemen
9.	Europäische Norm(en) und/oder europäische Normungsunterlage(n) zu Qualitätsmanagementsystemen für Anbieter von KI-Systemen, einschließlich Verfahren zur Beobachtung nach dem Inverkehrbringen
10.	Europäische Norm(en) und/oder europäische Normungsunterlagen zur Konformitätsbewertung für KI-Systeme

ANHANG II

Anforderungen an die europäischen Normen und europäischen Normungsunterlagen gemäß Artikel 1

1. Anforderungen an alle europäischen Normen und europäischen Normungsunterlagen

Europäische Normen und europäische Normungsunterlagen müssen den allgemein anerkannten Stand der Technik widerspiegeln, um Risiken für die Gesundheit und Sicherheit und die Grundrechte von Personen, wie sie in der Charta der Grundrechte der Europäischen Union und im geltenden EU-Recht zum Schutz der Grundrechte garantiert sind, zu minimieren, die sich aus der Konzeption und Entwicklung von KI-Systemen im Hinblick auf ihre Zweckbestimmung ergeben. Der Stand der Technik ist zu verstehen als ein zu einem bestimmten Zeitpunkt entwickelter Stand des technischen Könnens in Bezug auf Produkte, Verfahren und Dienstleistungen, der auf den einschlägigen gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung beruht und als gute Praxis in der Technik anerkannt ist. Der Stand der Technik bedeutet nicht zwangsläufig, dass sich die neueste wissenschaftliche Forschung noch im Versuchsstadium befindet oder technologisch noch nicht ausgereift ist. Um sicherzustellen, dass europäische Normen und europäische Normungsunterlagen mit dem Unionsrecht in Bezug auf die Grundrechte und den Datenschutz im Einklang stehen, müssen CEN und Cenelec einschlägiges Fachwissen in diesen Bereichen sammeln.

In den europäischen Normen und Normungsunterlagen sind – soweit angemessen und unbeschadet der Anforderungen dieses Anhangs und des Schutzes der EU-Werte und der Grundrechte von Personen, wie sie in der Charta der Grundrechte der Europäischen Union sowie im geltenden EU-Recht zum Schutz der Grundrechte garantiert sind – internationale Bestrebungen im Bereich der Normung zu berücksichtigen. Die europäischen Normen und europäischen Normungsunterlagen müssen mit dem Rechtsrahmen und den internationalen Verpflichtungen der Union im Einklang stehen.

Die europäischen Normen und europäischen Normungsunterlagen müssen im erforderlichen Umfang und unter Berücksichtigung des Stands der Technik technologie-, prozess- oder methodengestützte technische Spezifikationen für den Entwurf und die Entwicklung von KI-Systemen enthalten, einschließlich Überprüfungs-, Validierungs- und Testverfahren sowie objektiv nachprüfbarer Kriterien und praktikabler Methoden zur Bewertung der Einhaltung dieser Spezifikationen. Bei Bedarf sind auch unterstützende Spezifikationen, einschließlich solcher zur Terminologie, zu ermitteln und bereitzustellen, um die Kohärenz und die Fähigkeit zur Umsetzung der europäischen Normen und europäischen Normungsunterlagen zu gewährleisten. Alle auf der Grundlage dieses Auftrags erarbeiteten europäischen Normen und europäischen Normungsunterlagen müssen auf einer einheitlichen Terminologie beruhen. Die unterstützenden Spezifikationen zur Terminologie müssen so weit wie möglich auf der auf internationaler Ebene und insbesondere in internationalen Normen festgelegten Terminologie aufbauen.

Bei der Ausarbeitung der europäischen Normen und europäischen Normungsunterlagen müssen die gemeinsamen (horizontalen) Risiken von KI-Systemen, einschließlich der Systeme, die nach dem Inverkehrbringen oder der

Inbetriebnahme weiter dazulernen und die von der Kommission im Rahmen des Vorschlags für eine Verordnung mit harmonisierten Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) als mit Hochrisiko-KI-Systeme eingestuft worden sind, besonders berücksichtigt werden.

Ungeachtet ihres allgemeinen horizontalen Charakters können europäische Normen oder europäische Normungsunterlagen Spezifikationen enthalten, die sich auf bestimmte KI-Systeme (Anwendungsfälle) oder Sektoren beziehen (im Folgenden „vertikale Spezifikationen“), wobei die Zweckbestimmung und/oder der Kontext der Verwendung solcher Systeme zu berücksichtigen sind. Zwar ist es nicht immer möglich, europäische Normen und europäische Normungsunterlagen zu entwickeln, die jede spezifische Zweckbestimmung berücksichtigen, europäische Normen und europäische Normungsunterlagen müssen jedoch zumindest eine Reihe von technischen Lösungen und Optionen abdecken, die der Hersteller im Hinblick auf die Zweckbestimmung seines spezifischen Systems bewerten und umsetzen kann. Ferner sollten die europäischen Normen und europäischen Normungsunterlagen gegebenenfalls Leitlinien dazu enthalten, wie eine solche Bewertung und Umsetzung von Lösungen und Optionen durchzuführen sind.

In den Bereichen menschliche Aufsicht und Genauigkeit sind in den Abschnitten 2.5 und 2.6 spezifische Anforderungen an vertikale Spezifikationen festgelegt.

Die europäischen Normen und europäischen Normungsunterlagen müssen in angemessener Weise die Arbeiten des Europäischen Instituts für Telekommunikationsnormen (ETSI) berücksichtigen, insbesondere in Bezug auf:

- a) die Entwicklung der in Anhang I Nummer 8 genannten europäischen Normen und europäischen Normungsunterlagen und die Einbeziehung von Sicherheitsaspekten in die in Anhang I aufgeführten europäischen Normen und europäischen Normungsunterlagen, die nicht unter Nummer 8 genannt werden,
- b) die Entwicklung und nähere Ausarbeitung von möglichen vertikalen Spezifikationen,
- c) Test- und Validierungsverfahren für KI-Systeme.

Zu diesem Zweck sind CEN und Cenelec gehalten, geeignete Formen der Zusammenarbeit mit dem ETSI festzulegen.

In den erarbeiteten europäischen Normen und europäischen Normungsunterlagen müssen die Zusammenhänge zwischen den verschiedenen in Abschnitt 2 aufgeführten Anforderungen berücksichtigt werden und, soweit möglich, in den entsprechenden Spezifikationen ausdrücklich zum Ausdruck kommen.

CEN und Cenelec müssen sicherstellen, dass die erarbeiteten europäischen Normen und europäischen Normungsunterlagen gegebenenfalls mit den bestehenden und künftigen europäischen und allgemeinen Normen übereinstimmen, die in den verschiedenen einschlägigen Sektoren entwickelt werden, insbesondere mit denjenigen, die sich auf Produkte beziehen, die unter die bestehenden Sicherheitsvorschriften der Union, einschließlich der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit, fallen.

CEN und Cenelec müssen gebührend berücksichtigen, dass die Bereiche, die von den europäischen Normen und europäischen Normungsunterlagen abgedeckt werden, Gegenstand eines künftigen Normungsauftrags für harmonisierte Normen zur Unterstützung des Gesetzes über künstliche Intelligenz sein können.

CEN und Cenelec müssen sicherstellen, dass bei der Ausarbeitung der europäischen Normen und europäischen Normungsunterlagen die Besonderheiten und Kosten kleiner und mittlerer Unternehmen angemessen berücksichtigt werden, insbesondere in Bezug auf Qualitätsmanagementsysteme und Konformitätsbewertungen (Abschnitte 2.9 und 2.10).

2. Anforderungen an spezifische europäische Normen und europäische Normungsunterlagen

2.1 Risikomanagementsystem für KI-Systeme

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen Spezifikationen für ein Risikomanagementsystem für KI-Systeme festgelegt werden. Das Risikomanagement muss als kontinuierlicher, sich wiederholender Prozess während des gesamten Lebenszyklus des KI-Systems konzipiert sein, mit dem die entsprechenden Risiken für die Gesundheit, die Sicherheit oder die Grundrechte vermieden oder minimiert werden sollen.

Die Spezifikationen müssen so gestaltet sein, dass bei KI-Systemen, bei denen es sich um Sicherheitskomponenten von Produkten handelt oder die selbst Produkte sind, die mit dem KI-System zusammenhängenden Aspekte des Risikomanagementsystems gegebenenfalls in bestehende Risikomanagementsysteme integriert werden können, die zur Erfüllung der Anforderungen an Risikomanagementsysteme in den in Anhang II Abschnitt A des Vorschlags für ein Gesetz über künstliche Intelligenz aufgeführten Harmonisierungsrechtsvorschriften der Union eingerichtet wurden.

Die Spezifikationen sind so abzufassen, dass sie von den einschlägigen Betreibern und Marktüberwachungsbehörden verwendet werden können.

2.2 Daten und Daten-Governance

Diese europäische(n) Norm(en) oder europäische(n) Normungsunterlage(n) müssen:

- a) Spezifikationen für geeignete Daten-Governance- und Datenmanagementverfahren enthalten, die von den Anbietern von KI-Systemen umzusetzen sind (mit besonderem Schwerpunkt auf Datengenerierung und -erfassung, Datenaufbereitungsvorgängen, konzeptionellen Entscheidungen und Verfahren zur Erkennung und Behebung von Verzerrungen und potenzieller Diskriminierung durch Ersatzdaten („Proxy-Diskriminierung“) oder anderen relevanten Mängeln in den Daten) und
- b) Spezifikationen zu Qualitätsaspekten von Datensätzen enthalten, die zum Trainieren, Validieren und Testen von KI-Systemen verwendet werden (einschließlich Repräsentativität, Relevanz, Vollständigkeit und Korrektheit).

2.3 Aufzeichnung durch Protokollierungsfunktionen

Diese europäische(n) Norm(en) oder europäische(n) Normungsunterlage(n) müssen Spezifikationen für die automatische Protokollierung von Ereignissen für KI-Systeme enthalten. Diese Spezifikationen müssen die Rückverfolgbarkeit dieser Systeme während ihres gesamten Lebenszyklus und die Überwachung ihres Betriebs ermöglichen und die Beobachtung der KI-Systeme durch die Anbieter nach dem Inverkehrbringen erleichtern.

2.4 Transparenz und Informationen für die Nutzer

Diese europäische(n) Norm(en) oder europäische(n) Normungsunterlage(n) müssen Spezifikationen enthalten, die sich auf Folgendes beziehen:

- a) Konzeptions- und Entwicklungslösungen, die die Transparenz des Betriebs des KI-Systems gewährleisten, damit die Nutzer die Ergebnisse des Systems verstehen und angemessen nutzen können und
- b) Gebrauchsanweisungen für begleitende KI-Systeme mit Anweisungen zu den Fähigkeiten und Grenzen des Systems sowie zu Wartungs- und Pflegemaßnahmen, wobei insbesondere Folgendes zu berücksichtigen ist:
 - i) die Notwendigkeit, Informationen zu ermitteln und angemessen zu unterscheiden, die für verschiedene Profile beruflicher und anderer Nutzer relevant und verständlich sind, und
 - ii) unbeschadet der Ziffer i die Notwendigkeit, dafür zu sorgen, dass die ermittelten Informationen für die Nutzer ausreichend sind, um die Ergebnisse des Systems zu interpretieren und sie in einer Weise zu nutzen, die die Risiken mindert.

2.5 Menschliche Aufsicht

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen Maßnahmen und Verfahren für die menschliche Aufsicht über KI-Systeme festgelegt werden, die:

- a) vor dem Inverkehrbringen oder der Inbetriebnahme vom Anbieter bestimmt und, sofern technisch machbar, in das KI-System eingebaut werden und
- b) vor dem Inverkehrbringen oder der Inbetriebnahme des KI-Systems vom Anbieter bestimmt werden und dazu geeignet sind, vom Nutzer umgesetzt zu werden.

Dazu gehören Maßnahmen, die es den Nutzern ermöglichen, die relevanten Aspekte des Betriebs des KI-Systems zu verstehen, zu überwachen, zu interpretieren, zu bewerten und zu beeinflussen.

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen auch, soweit gerechtfertigt, geeignete Maßnahmen zur Aufsicht festgelegt werden, die für bestimmte KI-Systeme im Hinblick auf ihre Zweckbestimmung spezifisch sind. Bei KI-Systemen, die für die biometrische Fernidentifikation von Personen bestimmt sind, müssen die Maßnahmen der menschlichen Aufsicht so gestaltet sein, dass der Nutzer keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange dies nicht von mindestens zwei natürlichen Personen überprüft und bestätigt wurde.

2.6 Spezifikationen für die Genauigkeit von KI-Systemen

Für die Zwecke dieser europäischen Norm(en) oder europäischen Normungsunterlage(n) bezieht sich der Begriff „Genauigkeit“ auf die Fähigkeit des KI-Systems, die Aufgabe zu erfüllen, für die es konzipiert wurde. Dies ist nicht zu verwechseln mit der engeren Definition der statistischen Genauigkeit, die eine von mehreren möglichen Kennzahlen für die Bewertung der Leistung von KI-Systemen ist.

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen Spezifikationen festgelegt werden, die ein angemessenes Maß an Genauigkeit

von KI-Systemen gewährleisten und es den Anbietern ermöglichen, die Genauigkeitskennzahlen und den Genauigkeitsgrad anzugeben.

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen auch, soweit gerechtfertigt, eine Reihe geeigneter und relevanter Instrumente und Kennzahlen zur Messung der Genauigkeit anhand angemessen definierter Genauigkeitsgrade festgelegt werden, die für bestimmte KI-Systeme im Hinblick auf ihre Zweckbestimmung spezifisch sind.

2.7 Spezifikationen für die Robustheit von KI-Systemen

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen Spezifikationen für die Robustheit von KI-Systemen festgelegt werden, wobei relevante Ursachen für Fehler, Störungen und Unstimmigkeiten sowie die Wechselwirkungen des KI-Systems mit der Umgebung zu berücksichtigen sind.

2.8 Spezifikationen für die Cybersicherheit von KI-Systemen

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen geeignete organisatorische und technische Lösungen vorgesehen sein, damit KI-Systeme widerstandsfähig gegenüber Versuchen böswilliger Dritter sind, unter Ausnutzung der Schwachstellen der KI-Systeme deren Verwendung, Verhalten, Leistung oder Sicherheitsmerkmale zu verändern. Organisatorische und technische Lösungen müssen daher gegebenenfalls Maßnahmen zur Verhinderung und Beherrschung von Cyberangriffen umfassen, mit denen versucht wird, KI-spezifische Ressourcen wie Trainingsdatensätze (z. B. Datenvergiftung) oder trainierte Modelle (z. B. feindliche Beispiele) zu manipulieren oder Schwachstellen in den digitalen Ressourcen des KI-Systems oder der zugrunde liegenden IKT-Infrastruktur auszunutzen. Die technischen Lösungen müssen den jeweiligen Umständen und Risiken angemessen sein.

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen die grundlegenden Anforderungen an Produkte mit digitalen Elementen, wie sie in Anhang I Abschnitte 1 und 2 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen¹ aufgeführt sind, gebührend berücksichtigt werden.

2.9 Qualitätsmanagementsysteme für Anbieter von KI-Systemen, einschließlich Verfahren zur Beobachtung nach dem Inverkehrbringen

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) sind die Spezifikationen für ein Qualitätsmanagementsystem festzulegen, das die Anbieter von KI-Systemen in ihren Organisationen einführen müssen. Diese Qualitätsmanagementsysteme müssen unter anderen gewährleisten, dass ein KI-System fortlaufend die unter den Nummern 2.2, 2.3, 2.4, 2.5, 2.6, 2.7 und 2.8 beschriebenen Aspekte erfüllt. Die Umsetzung von Maßnahmen des Qualitätsmanagementsystems durch kleine und mittlere Unternehmen und Organisationen muss in angemessener Weise berücksichtigt werden.

¹ COM(2022) 454 final vom 15. September 2022.

Die Spezifikationen müssen so gestaltet sein, dass die Aspekte des Qualitätsmanagementsystems im Zusammenhang mit dem KI-System in das Gesamtmanagementsystem des Anbieters integriert werden können, insbesondere mit bestehenden Qualitätsmanagementsystemen, die zur Erfüllung der Anforderungen an Qualitätsmanagementsysteme in den in Anhang II Abschnitt A des Vorschlags für das Gesetz über künstliche Intelligenz aufgeführten Harmonisierungsrechtsvorschriften der Union eingerichtet wurden.

2.10 Konformitätsbewertung für KI-Systeme

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) müssen die Verfahren und Prozesse für die Konformitätsbewertung von KI-Systemen und Qualitätsmanagementsystemen von KI-Anbietern festgelegt sein.

Dabei müssen auch die Kriterien für die Bewertung der Kompetenz der mit der Konformitätsbewertung beauftragten Personen festgelegt werden.

In dieser (diesen) europäischen Norm(en) oder europäischen Normungsunterlage(n) sind verschiedene Szenarien zu berücksichtigen, bei denen die Konformitätsbewertung entweder vom Anbieter selbst oder unter Einbeziehung einer externen fachkundigen Stelle durchgeführt wird.