



DKE

KI – Made in Germany

DEUTSCHE NORMUNGS-
ROADMAP KÜNSTLICHE
INTELLIGENZ (AUSGABE 2)

**HANDLUNGSEMPFEHLUNGEN
ZUR KI-STANDARDISIERUNG**

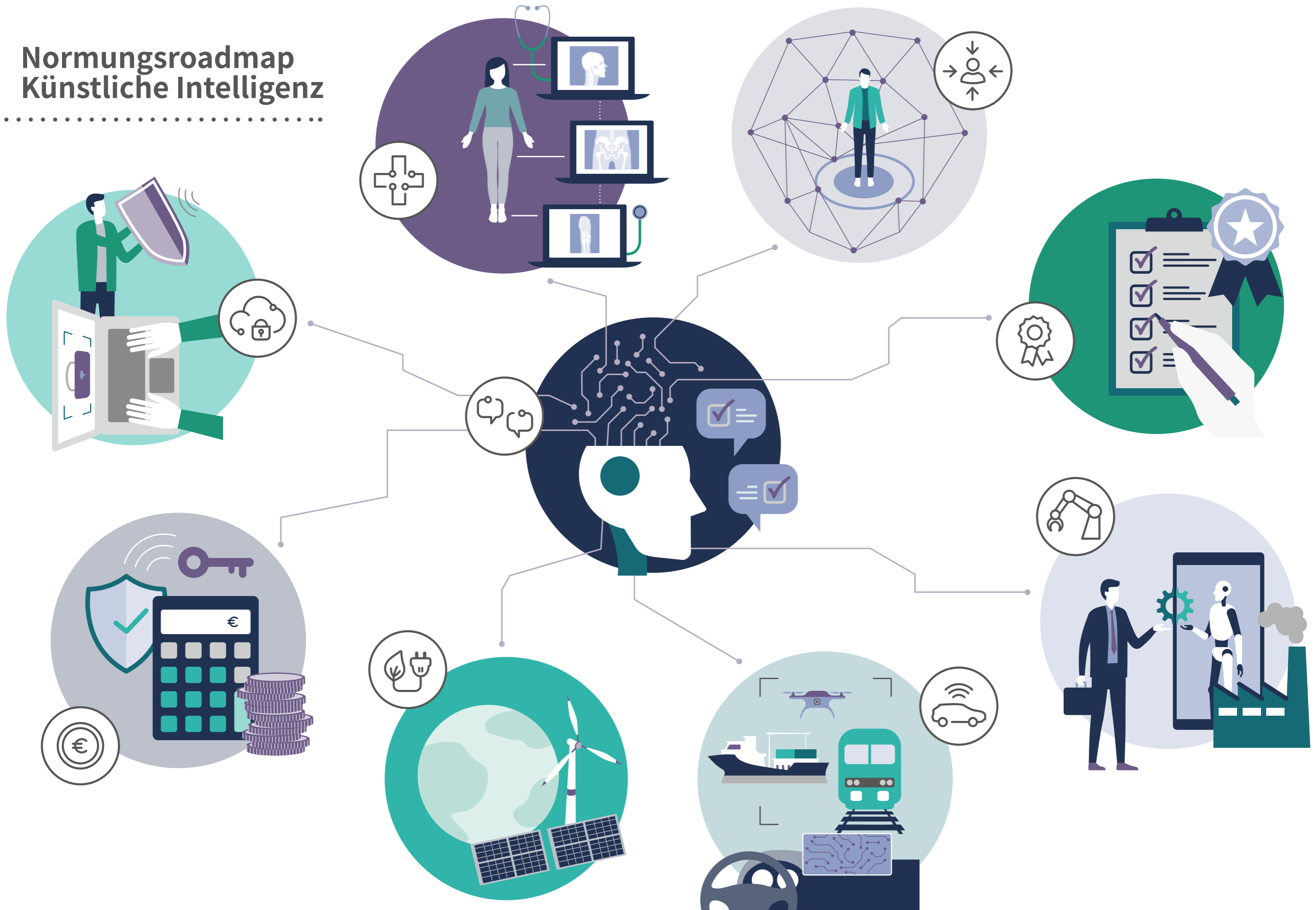
Eine Zusammenfassung

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

Normungsroadmap Künstliche Intelligenz



FÜR EINEN STARKEN KI-STANDORT DEUTSCHLAND

Normen und Standards stärken das Vertrauen von Wirtschaft und Gesellschaft in KI – die jetzt veröffentlichte zweite Ausgabe der Roadmap KI trägt dazu bei, indem sie weitere Bedarfe für Normen und Standards aufzeigt. Als Teil der KI-Strategie der Bundesregierung entwickelt sie den strategischen Fahrplan für die KI-Normung im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz weiter und gibt dazu konkrete Handlungsempfehlungen.

Roadmap unterstützt den AI Act

Mehr als 570 Fachleute aus Wirtschaft, Wissenschaft, öffentlicher Hand und Zivilgesellschaft haben den strategischen Fahrplan für die KI-Normung weiterentwickelt – begleitet von einer hochrangigen Koordinierungsgruppe für KI-Normung und -Konformität. Die Normungsroadmap KI zählt unter anderem auf den von der EU-Kommission veröffentlichten Entwurf zum Artificial Intelligence Act (AI Act) ein und identifiziert konkrete Bedarfe für Normen, die in Umsetzung des geplanten AI Acts zu erarbeiten sind.

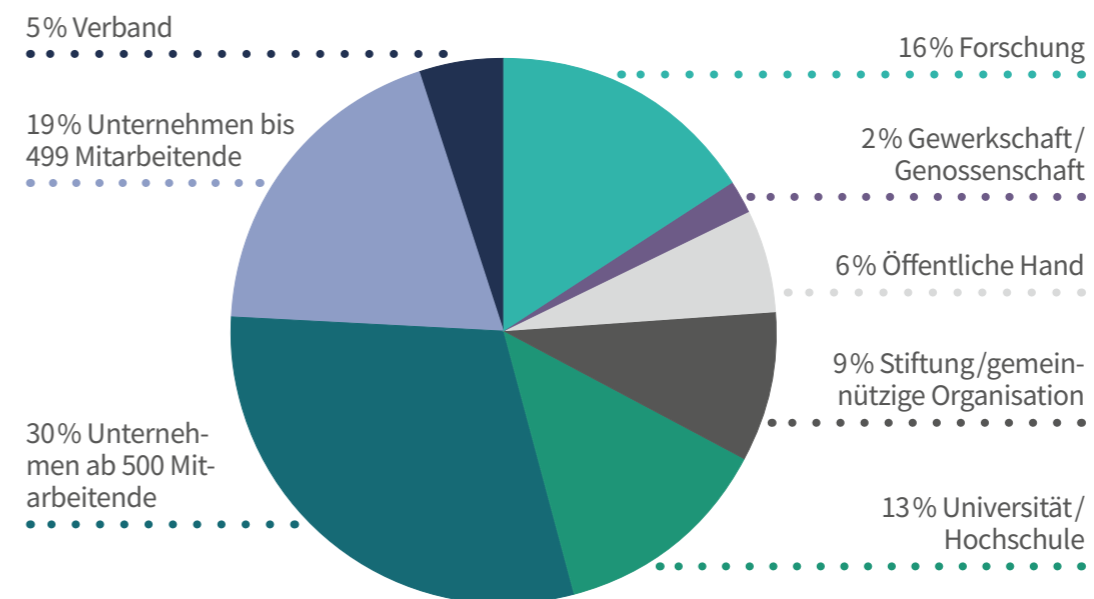
Innovationen voranbringen

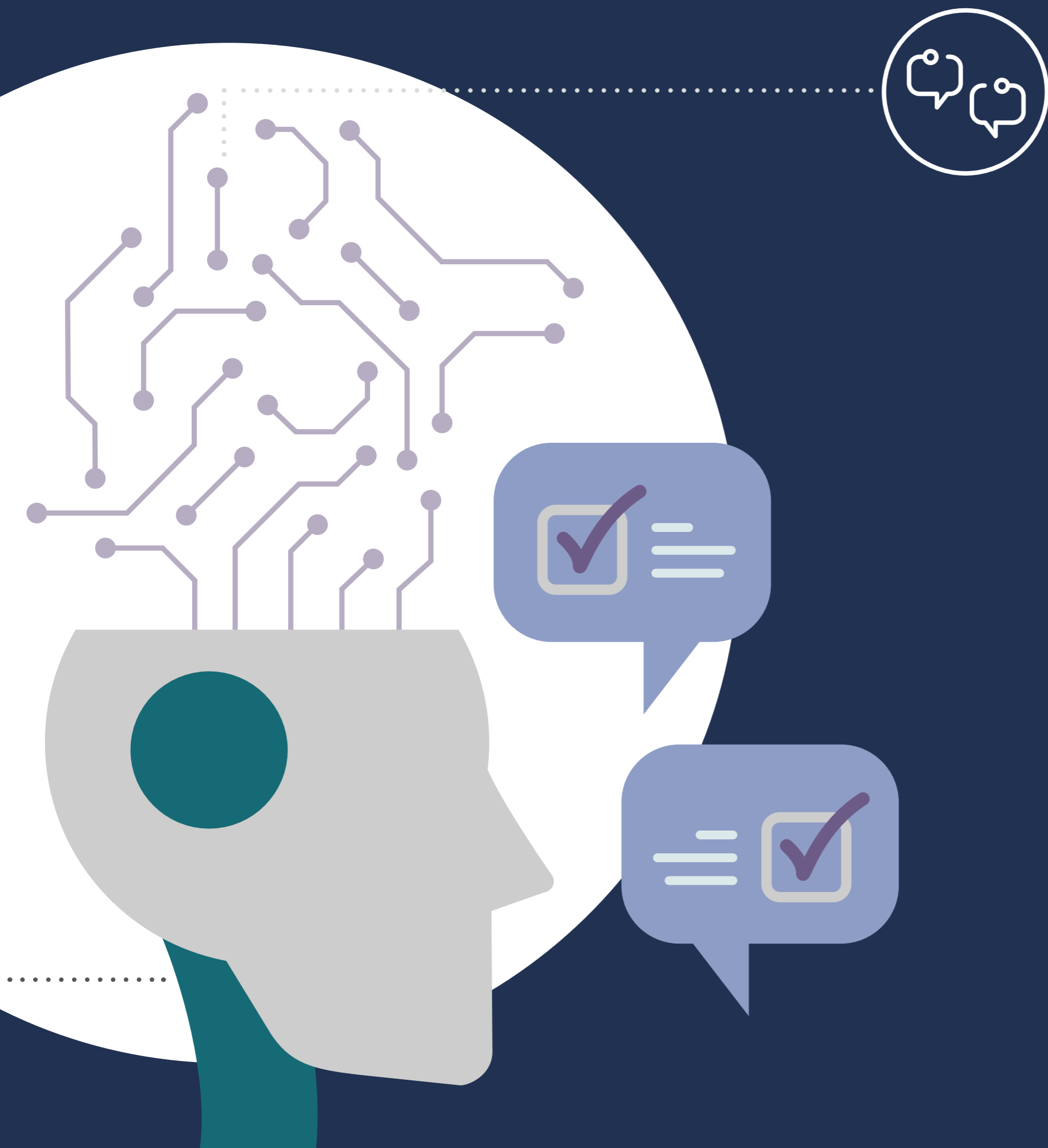
Insgesamt umfasst das Dokument 116 Normungs- und Standardisierungsbedarfe zu neun Schwerpunktthemen und liefert sechs zentrale Handlungsempfehlungen. Die Roadmap bildet den Startpunkt, um Normungs- und Standardisierungsaktivitäten anzustoßen. Mithilfe der entstehenden Normen und Standards werden innovationsfreundliche

Bedingungen für die Technologie der Zukunft geschaffen. Dafür sind fachkundige Expert*innen gefragt, die sich in den Normungsgremien engagieren. Die zweite Ausgabe der Normungsroadmap KI ist in neun Schwerpunktthemen unterteilt:

- Grundlagen
- Sicherheit
- Prüfung und Zertifizierung
- Soziotechnische Systeme
- Industrielle Automation
- Mobilität
- Medizin
- Finanzdienstleistungen
- Energie und Umwelt

Zusammensetzung der Mitwirkenden





Grundlagen

EINHEITLICHES VERSTÄNDNIS

Als Querschnittstechnologie bietet Künstliche Intelligenz großes Potenzial in vielen Branchen und Bereichen. Die Basis hierfür ist eine zuverlässige, funktionale und vor allem sichere KI. Die Normungsroadmap betrachtet Terminologien und bedeutsame Anwendungsgebiete wie Sprachtechnologien, bildgebende Sensorik, Quanten-KI und beschreibt KI-Methoden und -Fähigkeiten. Zudem werden ethische Prinzipien, Datenqualität und weitere Kriterien behandelt. All diese Themen sind die Grundlage für ein einheitliches Verständnis Künstlicher Intelligenz und lassen sich in Normen und Standards abbilden. Das fördert die Interoperabilität und das Zusammenwirken unterschiedlicher Systeme.

Sicherheit

BESTENS GESCHÜTZT

KI-Systeme müssen mehrfach sicher sein: Menschen, die mit einem KI-System interagieren, müssen geschützt sein (Safety). Außerdem dürfen die verwendeten Daten nicht missbraucht werden (Security). Nur eine tiefgehende Betrachtung der Sicherheit von KI-basierten Technologien und Anwendungen ermöglicht es, diese umfassend in Wirtschaft und Gesellschaft einzusetzen.

Derzeit besteht bei autonomen KI-Systemen noch die Herausforderung, Sicherheit für Leib und Leben nachweisen zu können. Die Normungsroadmap beschreibt eine Herangehensweise, um das Marktpotenzial entsprechender Anwendungen auszuschöpfen und die notwendige Risikoreduktion zu erreichen. Außerdem trägt sie dazu bei, das Marktpotential entsprechender Anwendungen auszuschöpfen und insbesondere die Schnittstellen zwischen Ethik, Recht und Technik bei Safety zu gestalten.

KI braucht zudem Vertrauen in Cybersecurity und Privacy. Prüfungen und Zertifizierungen können dazu beitragen, Normen und Standards sind wiederum Grundlage für Prüfungen und Zertifizierungen: Hier steht der Lebenszyklus der verwendeten Daten oder Algorithmen für KI-Systeme im Fokus.





Prüfung und Zertifizierung

AUF DEM PRÜFSTAND

KI-Systeme unterscheiden sich in vielerlei Hinsicht von herkömmlicher Software - Daten und Algorithmen nehmen eine viel zentralere Rolle ein. So sieht der geplante AI Act Prüfungen für KI-Anwendungen vor, die ein hohes Risiko für Gesundheit, Sicherheit oder Persönlichkeitsrechte haben können. Insbesondere der Qualitätsanspruch beispielsweise an die technische Zuverlässigkeit sowie die Erklärbarkeit und Nachvollziehbarkeit der KI-Anwendungen ist hier ganz zentral.

Um das Vertrauen in KI-Anwendungen zu stärken, sind Qualitätskriterien und Prüfverfahren notwendig, die KI-Systeme technisch beschreiben und messbar machen. Normen und Standards beschreiben Anforderungen an Kriterien und Verfahren (etwa hinsichtlich der Qualität, der Sicherheit und Transparenz) und sind damit Grundlage für die Zertifizierung von KI-Anwendungen. Zertifizierungen können so auch die Etablierung einer vertrauenswürdigen Marke „KI made in Europe“ voranbringen und damit die internationale Wettbewerbsfähigkeit Europas im Bereich KI stärken. Die Normungsroadmap empfiehlt, hierfür einen horizontalen KI-Qualitätsstandard zu entwickeln, der die Basis für weitere branchenspezifische Prüfungen und Zertifizierungen sein kann.

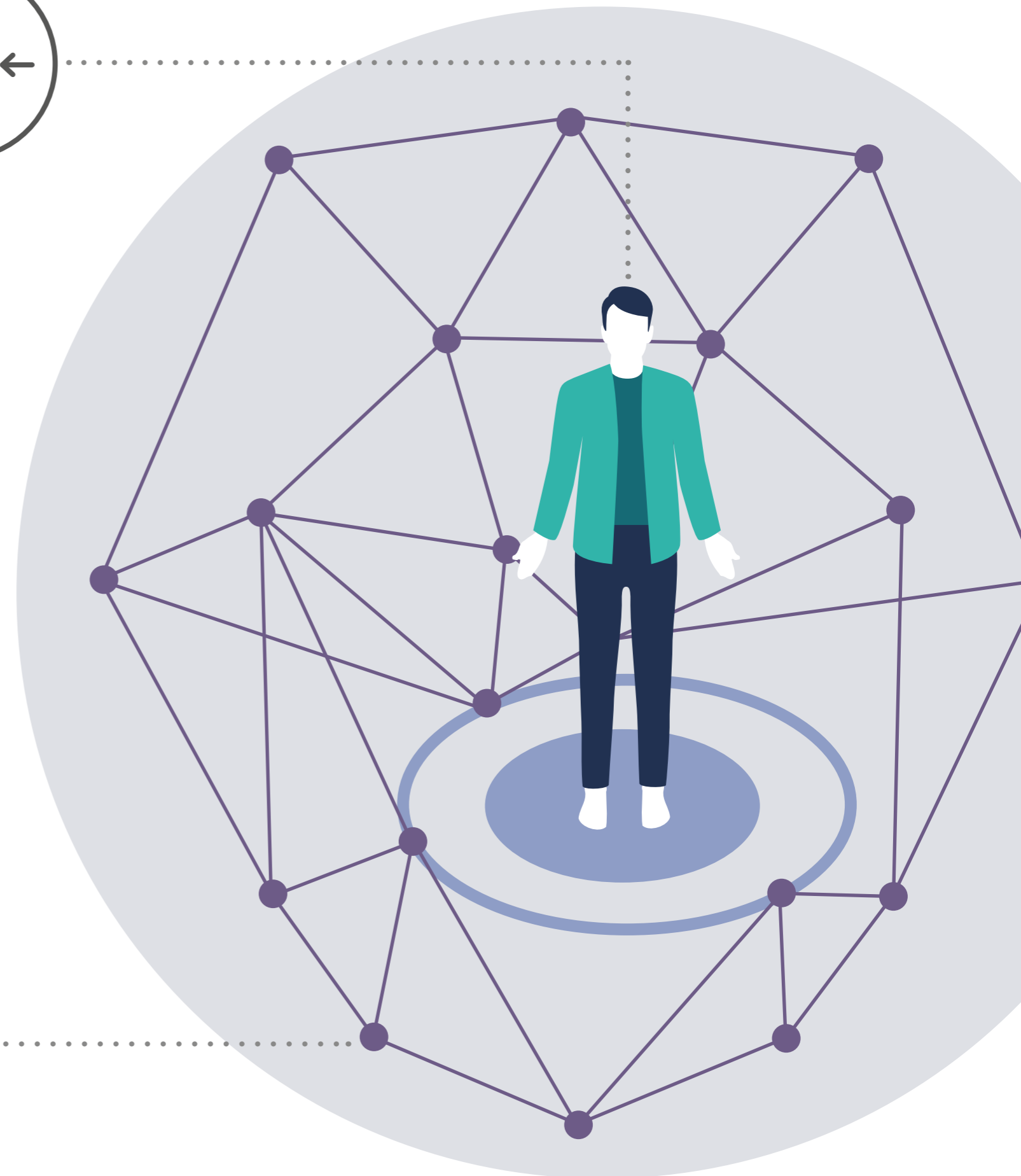
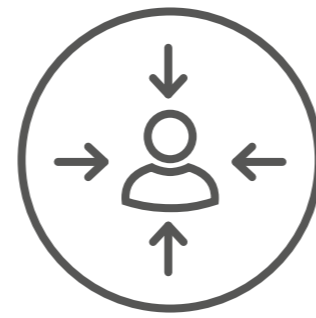


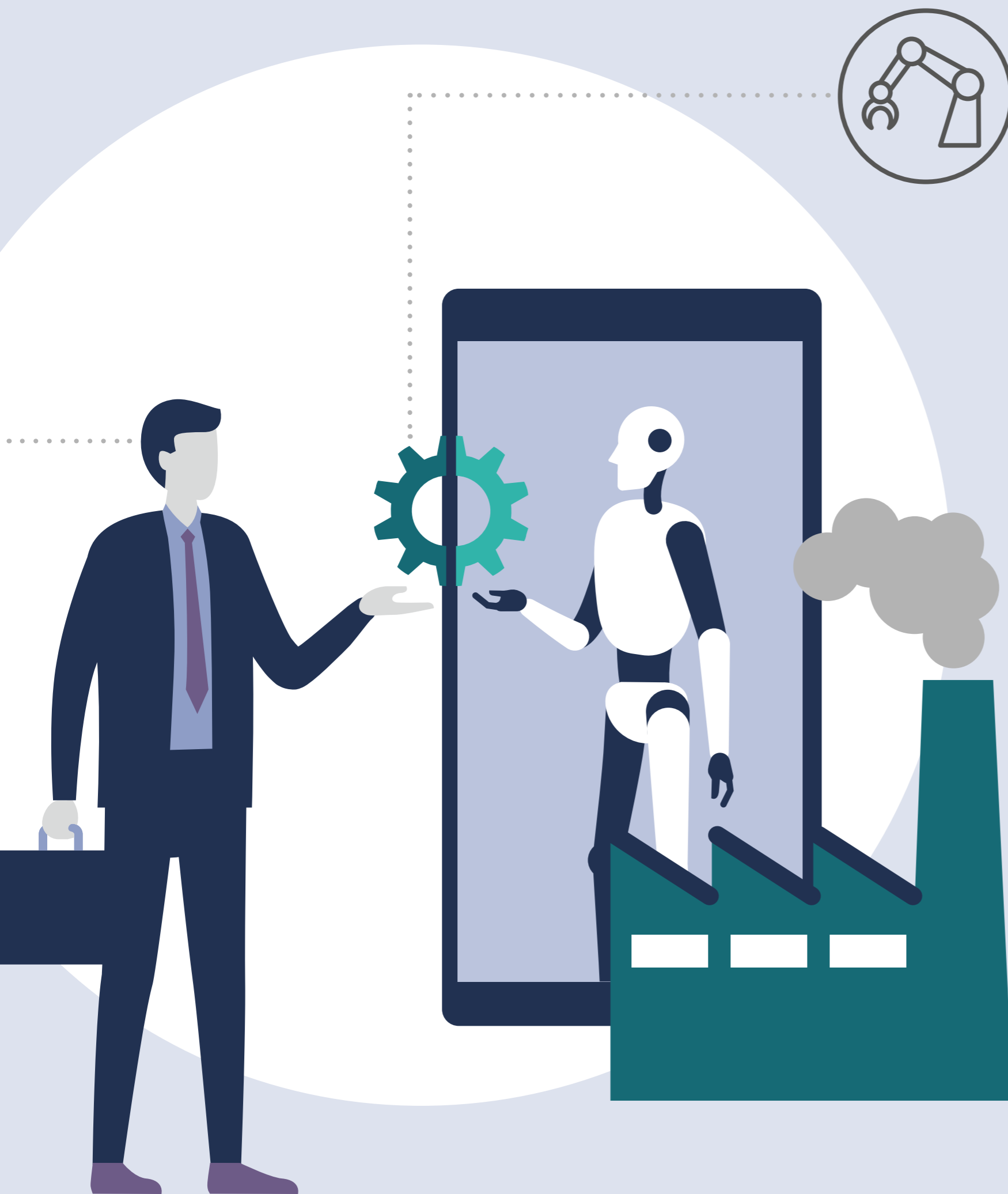
Soziotechnische Systeme

DER MENSCH IM MITTELPUNKT

KI steht immer im Kontext zum Menschen und zum organisatorischen Umfeld. Für erfolgreiche KI-Lösungen darf es deshalb nicht nur den Blick auf die Technologie geben. Vielmehr ist auch das soziotechnische System zu betrachten, in dem Künstliche Intelligenz eingesetzt wird und mit dem Menschen in Wechselwirkung steht. Ziel ist es, die Bedürfnisse der Nutzer*innen zu erkennen und die KI so zu gestalten, dass sie die Nutzer*innen bestmöglich bei ihren Aufgaben unterstützt. Insbesondere kleinen und mittelständischen Unternehmen sowie Start-ups soll es ermöglicht werden, KI-Technologien in ihre Geschäftsmodelle zu integrieren. Aufgabe der Normung ist es, alle relevanten Personengruppen und Blickwinkel unter Berücksichtigung soziotechnischer Aspekte einzubeziehen.

Im Verordnungsentwurf des AI Act spielen unter anderem die menschliche Aufsicht und Eingriffsmöglichkeit sowie die Transparenz in KI-Systemen bedeutende Rollen. Technische und soziale Komponenten sind deshalb vom Menschen aus zu denken und bei der Entwicklung darauf auszurichten.





Industrielle Automation

INTEGRIEREN UND INTERAGIEREN

Künstliche Intelligenz ist eine Schlüsseltechnologie, wenn es um die digitale Transformation des produzierenden Gewerbes geht. Eine wichtige Funktion wird dabei der digitalen Abbildung der physischen Realität zugeschrieben, dem digitalen Zwilling. Die Normungsroadmap stellt aktuelle Herausforderungen im Zusammenhang mit Datenmodellen für den Einsatz von KI in der industriellen Automation dar. Die Roadmap befasst sich außerdem damit, wie Mensch und Maschine interagieren und wie sich KI-Systeme integrieren lassen.

In der industriellen Automation sind Normen und Standards essenziell: Sie fördern die unternehmensübergreifende Interoperabilität und helfen dabei, regulatorische Rahmenbedingungen umzusetzen.

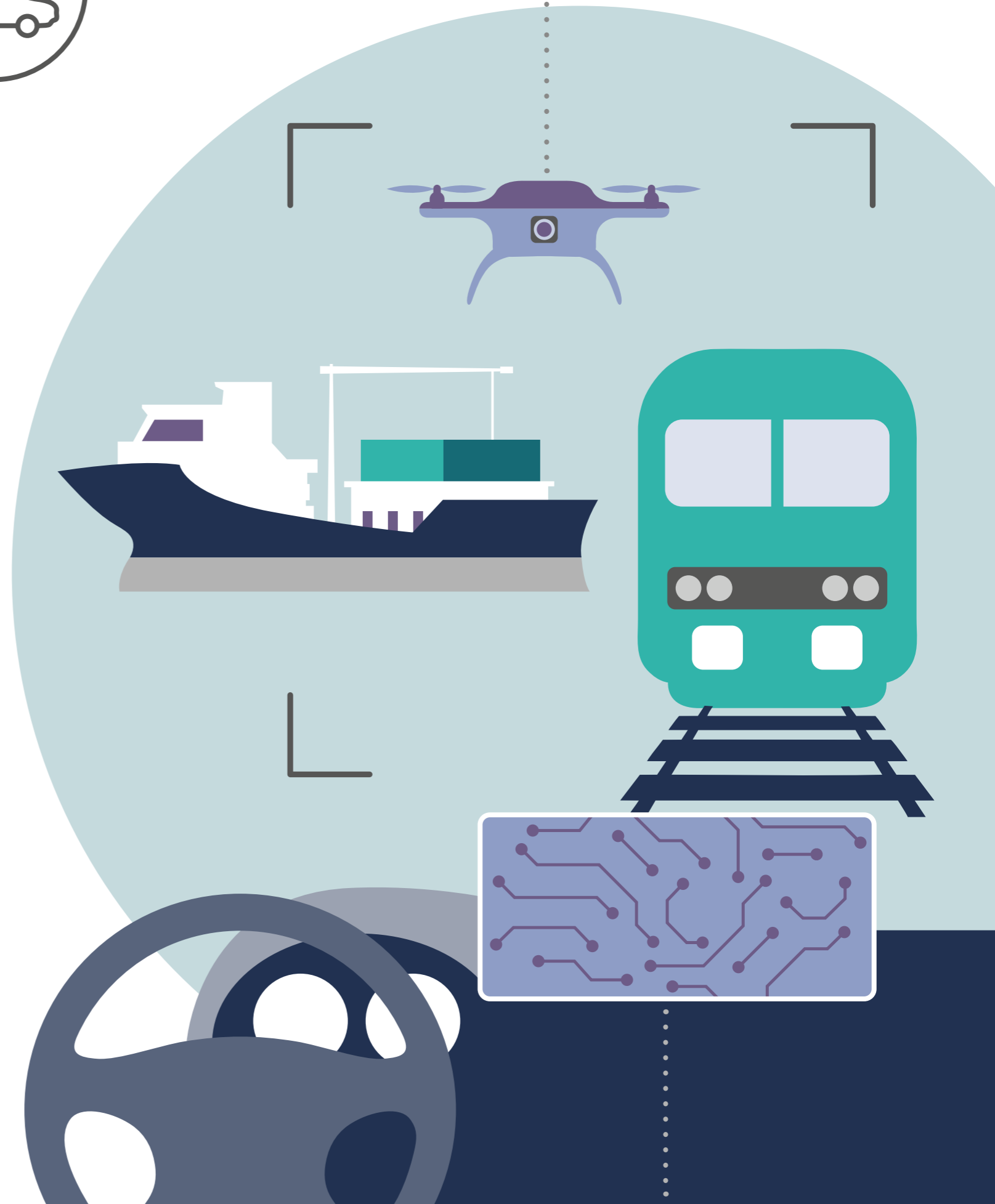
Mobilität

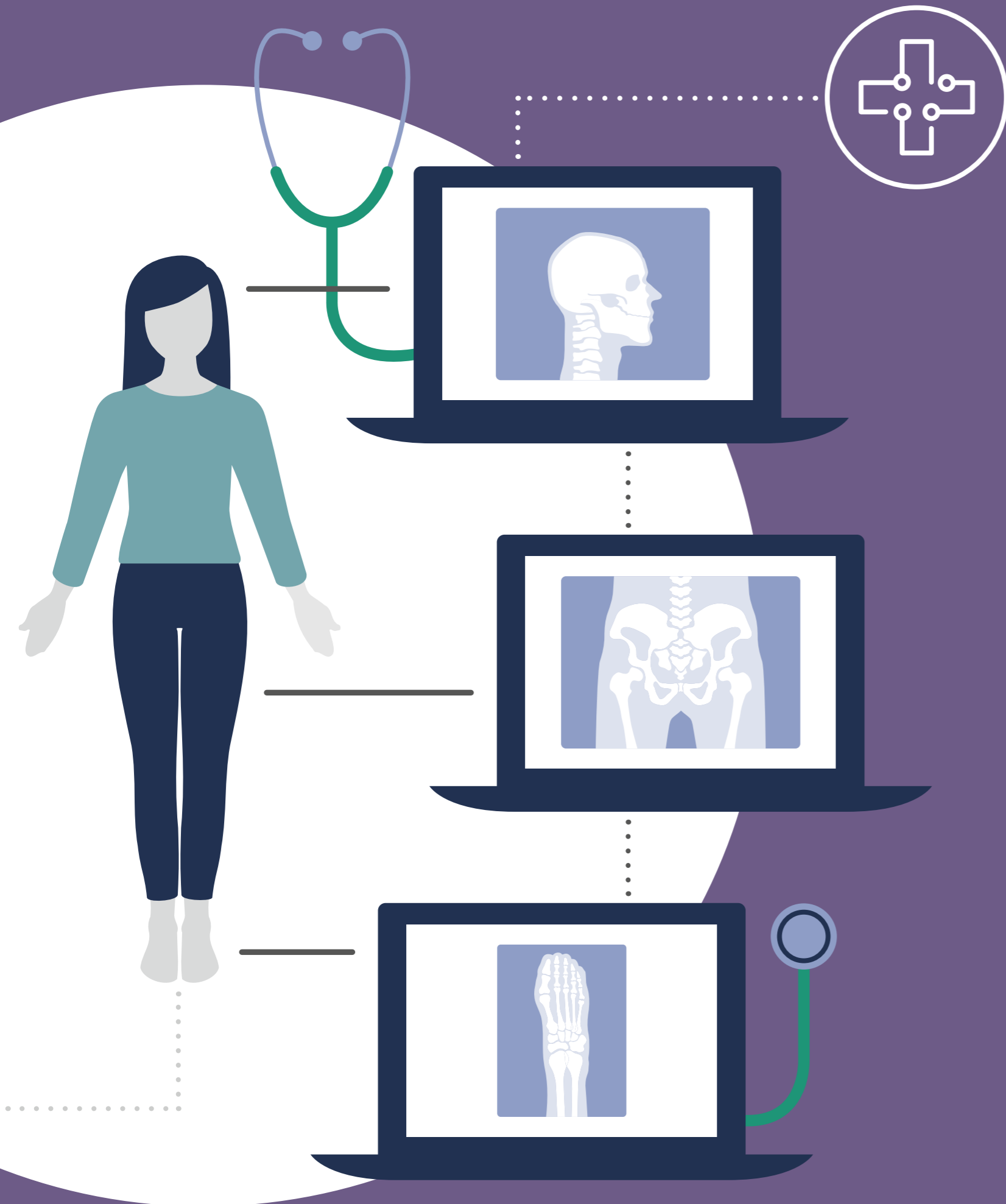
CLEVER STEUERN

Im Mobilitätssektor bietet der Einsatz Künstlicher Intelligenz viele Vorteile – beispielsweise, wenn selbstlernende Systeme komplexe automatisierte Steuerungsfunktionen übernehmen sowie Verkehrsströme oder Mobilitätsketten optimieren.

Normen und Standards für den Mobilitätsbereich können unter anderem:

- eine Grundlage zur Operationalisierung des geplanten AI Acts bilden, in dem sie objektive Methoden zur prüf-
baren Entwicklung nach „Trustworthiness-by-Design“ ermöglichen
- die dynamische, kontinuierliche (Re-)Zertifizierung beziehungsweise Typzulassung im Sinne einer kontinuierlichen Systementwicklung unterstützen
- Schnittstellen und Mindestanforderungen für die Interoperabilität, den Datenaustausch sowie die Trustworthiness und Safety bei automatisierten Mobilitätssystemen festlegen





Medizin

GESUNDES VERTRAUEN

Aus der Medizin der Zukunft wird KI nicht mehr wegzudenken sein – ob bei Diagnose, Therapie, Früherkennung oder im Pflegealltag. Zugleich ist der Einsatz der Technologie in diesem Bereich herausfordernd: Es geht nicht nur um die Gesundheit und persönliche Daten, sondern auch darum, Menschen schnell und sicher am medizinischen Fortschritt teilhaben zu lassen.

Normen und Standards können helfen:

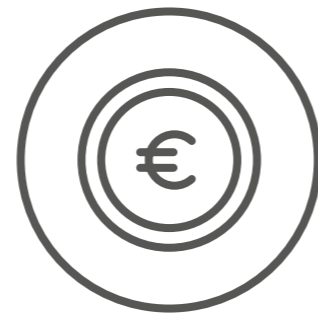
- die Nutzbarkeit und Verwertbarkeit von Daten für KI-basierte Systeme in der Medizin zu erhöhen
- die Leistungsfähigkeit und Sicherheit KI-basierter Medizinprodukte zu überprüfen
- Vertrauen und Akzeptanz bei Anwender*innen und Patient*innen zu schaffen
- die Qualitätsinfrastruktur regulatorischer Rahmenbedingungen für KI in Medizinprodukten effizient umzusetzen

Finanzdienstleistungen

SICHER UND FAIR

Money makes the world go round: Finanzdienstleistungen sichern soziale Teilhabe für alle und sind zugleich anspruchsvolle und hoch sensible Produkte – besonders in einer digitalisierten Welt. Bargeld wird schon seit langem durch reine Datenströme ersetzt, wie geschaffen für die Nutzung Künstlicher Intelligenz.

Wie lassen sich die neuen Möglichkeiten verantwortungsvoll nutzen, ohne die Risiken zu übersehen? Können Modelle für das Kundenverhalten zu Datenlecks werden? Welche Daten dürfen für Entscheidungsmodelle verwendet werden, und wie bestimmt man, wann genügend Informationen für faire Entscheidungen verfügbar sind? Wie finden sich KI-Modelle im klassischen Risikomanagement der Banken wieder? Das zu beantworten, wird durch Normen und Standards wesentlich vereinfacht.





Energie und Umwelt

NACHHALTIG VERSORGT

Energie ist Teil der kritischen Infrastruktur, insbesondere die Energiewende ist ein wichtiges politisches Thema. Wirtschaftlichkeit, Versorgungssicherheit, Klimaschutz und die Umstellung auf erneuerbare Energien stehen zugleich auf der Agenda. Künftig werden intelligente Stromnetze – Smart Grids – immer wichtiger. Sie verbinden Energietechnik mit Informations- und Kommunikationstechnologien. In dieses System aus Datenmodellen und Systemarchitekturen muss sich Künstliche Intelligenz integrieren.

KI ist darüber hinaus ein bedeutendes Instrument, um die von den Vereinten Nationen definierten 17 Ziele für nachhaltige Entwicklung zu erreichen. KI bietet Nutzungspotenziale im Kontext des European Green Deal. Mithilfe Künstlicher Intelligenz lassen sich beispielsweise sektorübergreifend Verhaltensempfehlungen für Marktakteur*innen und Verbraucher*innen entwickeln, um den ökologischen Fußabdruck zu minimieren. KI kann im Umweltbereich zudem ein Werkzeug für mehr Ressourceneffizienz in der Industrie sowie zur Verarbeitung großer Datenmengen in verschiedenen Wirtschaftssektoren sein. Normung leistet dabei einen Beitrag zum Umbau Deutschlands hin zum klimaneutralen Industrieland.

Handlungsempfehlungen der
Normungsroadmap KI

„KI MADE IN GERMANY“ VORANBRINGEN

Normen und Standards können zu sicherer, qualitativ hochwertiger, zuverlässiger und erklärbarer KI beitragen: Sie schaffen die Grundlagen für technische Souveränität, fördern Transparenz und bieten Orientierung. Um dieses Potenzial auszuschöpfen, liefert die Normungsroadmap KI mit der zweiten Ausgabe sechs übergreifende, zentrale Handlungsempfehlungen.

1.

Horizontales Konformitätsbewertungs- und Zertifizierungsprogramm für vertrauenswürdige KI entwickeln

Wie lassen sich die Anforderungen von Wirtschaft, Behörden und Zivilgesellschaft an KI objektiv überprüfbar machen? Für das wirtschaftliche Wachstum und die erfolgreiche Nutzung von KI-Systemen unter Berücksichtigung der europäischen Wertevorstellungen braucht es ein Konformitätsbewertungs- und Zertifizierungsprogramm. Anhand von verlässlichen und reproduzierbaren Prüfungen werden Aussagen zur KI-Vertrauenswürdigkeit belastbar.

2.

Dateninfrastrukturen und -qualitätsstandards zur Entwicklung und Validierung von KI-Systemen aufsetzen

Die Qualität eines KI-Systems hängt oft von der Qualität der verwendeten Daten ab. Inwiefern die deutsche KI-Industrie und insbesondere Start-ups auf entsprechende Datensätze zugreifen können, ist somit ein strategischer Wettbewerbsfaktor. Deshalb sind geeignete Infrastrukturen erforderlich, die Datensätze sammeln, beschreiben und bereitstellen. Normen und Standards stellen Interoperabilität sicher und legen Anforderungen an die Qualität fest.

3.

Den Menschen in allen Phasen des KI-Lebenszyklus als Teil des Systems begreifen

Welche Transparenz ist in welchem Kontext für welche Zielgruppe ausreichend? Wie lässt sich bei KI-Systemen die menschliche Aufsicht umsetzen? Und welche Informationen müssen als Grundlage für menschliche Eingriffe ins System vorhanden sein? All das sind Fragen, die vom Menschen aus zu denken und wonach die technischen und sozialen Komponenten zu entwickeln und auszurichten sind. In Leuchtturmprojekten ist konkret zu erproben, wie sich betroffene und beteiligte Menschen in alle Phasen des KI-Lebenszyklus einbinden lassen. Begleitend sind Normen für die soziotechnischen Aspekte des geplanten AI Act zu erarbeiten – hier kommt es besonders darauf an, dass alle relevanten Zielgruppen ausgewogen beteiligt sind. Zudem sollte die in der Normung bislang unterrepräsentierte soziotechnische Perspektive durch Fachleute ausgebaut werden.

4.

Vorgaben für die Konformitätsbewertung kontinuierlich lernender Systeme im Bereich der Medizin erarbeiten

Lernende KI-Systeme in der Medizin können beispielsweise über neue Trainingsdaten, Informationen von Fehlverhalten und gewonnenen Korrekturen kontinuierlich verbessert werden. Gleichzeitig müssen die entsprechend hohen Sicherheitsansprüche erfüllt werden. Dies erfordert eine (Re-)Konformitätsbewertung mit geeigneten Prüfverfahren. Um den Marktzugang für derartige Prüfverfahren zu ebnen, fordert die Roadmap Randbedingungen zu spezifizieren, die eine automatisierte Freigabe von kontinuierlich lernenden Systemen zulässt.

Hierfür wird die Initiierung von medizinspezifischen Teilprojekten unter Zusammenarbeit der relevanten Akteur*innen empfohlen, um die Projektergebnisse in Normen, Standards und allgemein praktikierbare Prüfverfahren zu überführen.



5.

Über Best Practices sichere und vertrauenswürdige KI-Anwendungen in der Mobilität entwickeln

Der Einsatz von KI-Technologien im Kontext der Mobilität ist gekennzeichnet durch komplexe Randbedingungen: Interagiert wird mit einer sich stetig ändernden Umwelt und vielen weiteren Akteur*innen. Fehlfunktionen können hohe Risiken für Mensch und Umwelt haben. Deshalb sind vertrauenswürdige KI-Systeme wichtig: Der geplante AI Act gibt verschiedene Aspekte von Vertrauenswürdigkeit vor. Diese sind anhand von Normen und Standards über den gesamten Lebenszyklus eines KI-Systems zu konkretisieren. Ein Best Practice-Katalog sollte dabei unterstützen, die Systeme im Betrieb effizient zu entwickeln und abzusichern. Die Roadmap empfiehlt außerdem, Normen und Standards zu erarbeiten, die Mindestanforderungen definieren, insbesondere an Safety und an wesentliche Vertrauensaspekte.



6.

Übergreifende Datenstandards und dynamische Modellierungsverfahren erarbeiten

Um Datensystemgrenzen zu überwinden und Referenzverfahren zu entwickeln, braucht es Normen und Standards. Die Normungsroadmap empfiehlt dafür folgende Pilotprojekte:

- Aufbau einer gemeinsamen Terminologie, Semantik, Taxonomie sowie darauf gestützte Datenmappings und -schemata in den Domänen Materialwissenschaften/Bauwesen zur Ermittlung von Energieeffizienz und Umweltwirkungen
- Entwicklung eines branchenunabhängigen Kommunikationsformats, um den Energie- und Ressourcenverbrauch von Gütern und Dienstleistungen zu bestimmen
- Entwicklung einer Methodik zur Beurteilung der Laufzeit, Akkuranz und Nachhaltigkeitsgüte von KI-Systemen



DKE

Nehmen Sie Kontakt auf!

Sie haben Fragen oder Anregungen
oder wollen selbst in der KI-Normung
aktiv werden?

Dann wenden Sie sich an:
Kuenstliche.Intelligenz@din.de

Die vollständigen Empfehlungen und Handlungsbedarfe sind in der
Deutschen Normungsroadmap KI (Ausgabe 2) zu finden: www.din.de/go/normungsroadmapki