100 YEARS SECURING THE FUTURE 1925 – 2025

# Perspektiven der TIC-Branche

## Vertrauen in Innovationen schaffen – digitale Infrastrukturen schützen

# Agenda

I. DEKRA im Überblick

II. Chancen und Risiken digitaler Technologien

III. Perspektiven für die Zukunft

IV. Vertrauen ermöglicht Innovationen

V. KI im Gesundheitswesen: Brustkrebserkennung

VI. DEKRA Prüfung von KI für Innovationen und Verbraucherschutz

VII. Klarer gesetzlicher Rahmen für ein vertrauensbasiertes Level Playing Field

VIII. Marktüberwachung im digitalen Kontext: AI Act

IX. Übersicht KI relevante Standards

X. Fazit

# I. DEKRA im Überblick: Sicherheit seit 100 Jahren – Securing the Future

## Gegründet im Jahr

# 1925

um „die **Verkehrssicherheit** im Zuge der rasant wachsenden Mobilität zu gewährleisten.“

Was 1925 mit der Überprüfung von Fahrzeugen begann, ist heute ein umfassendes Leistungsportfolio in den Bereichen Mobilität, Industrie, Umwelt und digitale Technologien. DEKRA prüft sowohl physische als auch digitale Produkte, Prozesse und Systeme.


DEKRA,
Deutschland, Berlin 1925

DEKRA,
Deutschland, Stuttgart 2025

## Meilensteine

**1960** – Zugelassen als Fahrzeugprüf-organisation

**1961** – Anerkannt als Überwachungs-organisation

**2005** – Start des Industrie-sicherheits-geschäfts

**2009** – Eintritt in den Markt für Produkt-zertifizierung

**2016** – Prüfung autonomes Fahren und vernetzte Mobilität – Málaga, Spanien

**2017** – Investition in das größte unabhängige Prüfzentrum für autonomes und vernetztes Fahren in Europa (Klettwitz, Deutschland)

**2018** – Ausbau der Cybersecurity-dienstleistungen

**2023** – Einstieg in die Prüfung von KI-Lösungen und Entwicklung KI-basierter Services für Prüfung und Zertifizierung

# I. DEKRA im Überblick: Strategie 2030+

**Strategisches Wachstum weltweit** durch **Innovation** und **Relevanz** in sich wandelnden Märkten. DEKRA bleibt führend in den **Kerndienstleistungen** und nutzt die steigende Nachfrage in Bereichen wie **Infrastrukturmodernisierung**, **Nachhaltigkeit** und **Sicherheitstechnologien** – mit Lösungen wie **Digital Trust** und **globaler Expertise**.

Zukunftssicheres Geschäftsmodell dank neuer Dienstleistungen und globaler Aufstellung

Strategische Transformation hin zu einem digitalen und softwaregetriebenen Mobilitätsexperten

## Future Mobility

- **Weltmarktführer in Fahrzeugprüfungen**
- **Automatisiertes & vernetztes Fahren**
- **Elektromobilität: Batterie- und Fahrzeugtests, Ladeinfrastruktur-Zertifizierung**, Hochvolt-Schulungen (~500 Batterietests/Monat 2024)
- **Batterietestzentrum Klettwitz**
- **Cybersecurity** für Fahrzeugsysteme

## Sustainability

- **500+ Services** für Nachhaltigkeit & Compliance, maßgeschneidert für alle Branchen und Größen
- Abdeckung des gesamten Tech-Lebenszyklus: Planung, Produktion, Betrieb, Recycling
- Unterstützung bei **Energiewende, ESG und Kreislaufwirtschaft**
- **Beratung, Prüfung, Zertifizierung, Audits, Training**
- Ausgerichtet an **EU Green Deal, REPowerEU, EU-Taxonomie**


## Weltweit erster „Digital-Trust“ Service

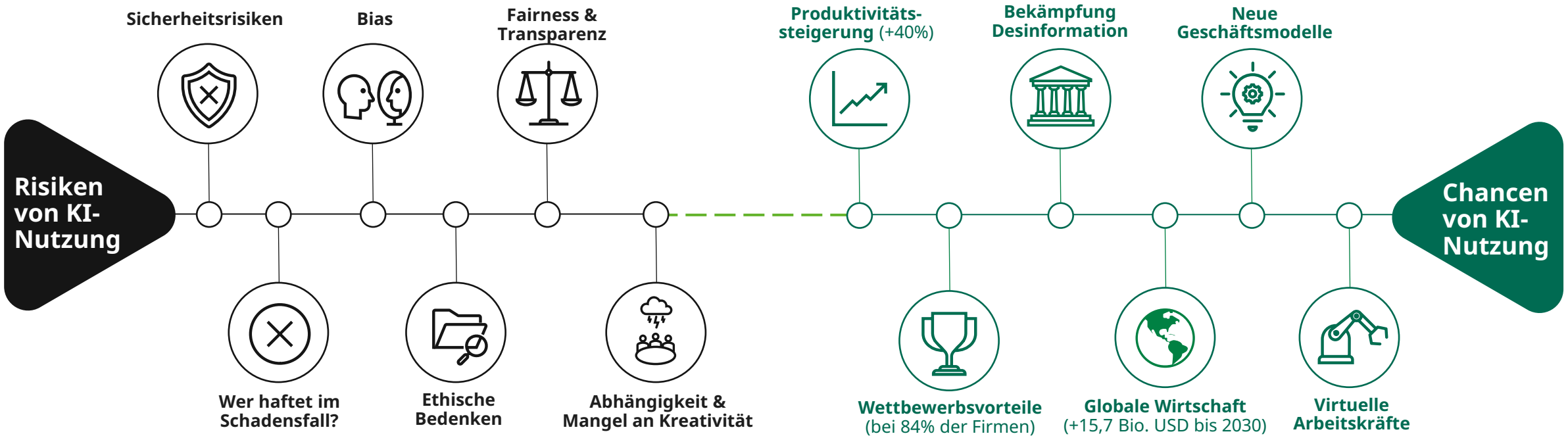
- **Cybersicherheit, funktionale Sicherheit** und **KI-Compliance** zusammengefasst
- **Weltweite Prüfung** & Zertifizierung mit **200+ Experten** im Bereich Digital Trust
- **Innovation beschleunigen, Markteintritt verkürzen** – mit **einem vertrauenswürdigen Partner**

## Defense / Aerospace

- Automotive (Transport & Logistik)
- Informations- und Cybersicherheit
- Training
- Industrieprüfungen

# II. Chancen und Risiken digitaler Technologien

Fokus Künstliche Intelligenz



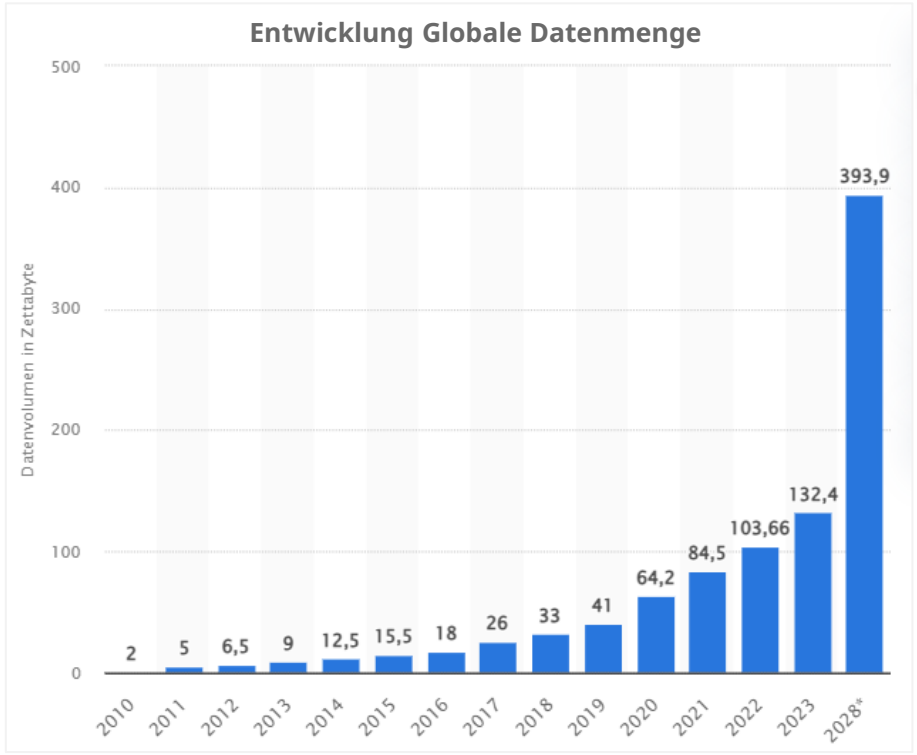

**Künstliche Intelligenz hat ein enormes Potenzial:** positive Auswirkungen auf das globale Wirtschaftswachstum, Verbesserungen bei der Arbeitsproduktivität, Durchbrüche im Bereich Forschung und Entwicklung, u.v.m.

**Gleichzeitig kann KI-Technologie selbst signifikante Risiken bergen,** insbesondere bei der Anwendung in sicherheitskritischen Bereichen – aber auch für die Grundrechte und die Demokratie.

# II. Chancen und Risiken digitaler Technologien

Digitalisierung: Wo stehen wir?

Die weltweite Datenmenge wächst exponentiell – und mit ihr die Angriffsfläche für Cyberbedrohungen




Statista 2024


Laut dem Global Risk Report 2025 zählen technologische Risiken zu den schwerwiegendsten

**Top 10 Globale Risiken bis 2035**

| | |
|---|---|
| 1st | Extreme weather events |
| 2nd | Biodiversity loss and ecosystem collapse |
| 3rd | Critical change to Earth systems |
| 4th | Natural resource shortages |
| 5th | Misinformation and disinformation |
| 6th | Adverse outcomes of AI technologies |
| 7th | Inequality |
| 8th | Societal polarization |
| 9th | Cyber espionage and warfare |
| 10th | Pollution |

World Economic Forum 2025

# III. Perspektiven für die Zukunft

Wege zur sicheren, resilienten und nachhaltigen digitalen Infrastruktur

## ZENTRALE TRENDS & TREIBER

### Technologische Dynamik

- Neue Prüfmethoden für KI, Cybersecurity & Blockchain
- Wachsender Bedarf im digitalen Raum durch rasante Innovation

### Regulatorische Entwicklung

- EU AI Act, CRA, NIS-2
- Frühe Prüfungen, Standardisierung, internationale Harmonisierung

### Zusammenarbeit im Digitalen Ökosystem

- Politik, Wirtschaft, Forschung und die TIC-Branche
- Gemeinsame Standards entwickeln & Pilotprojekte

### Neue Wertedimensionen

- Nachhaltigkeit und Resilienz digitaler Systeme als Wettbewerbsvorteil

## ROLLE VON DEKRA

1. Vertrauenswürdiger, unabhängiger Partner für Sicherheit und Qualität
2. Pionierrolle bei Prüfmethoden für KI, Cybersicherheit und vernetzten Systemen
3. Schnittstelle zwischen Regulierung und Industrie für eine sichere und schnelle Markteinführung digitaler Systeme und Produkte

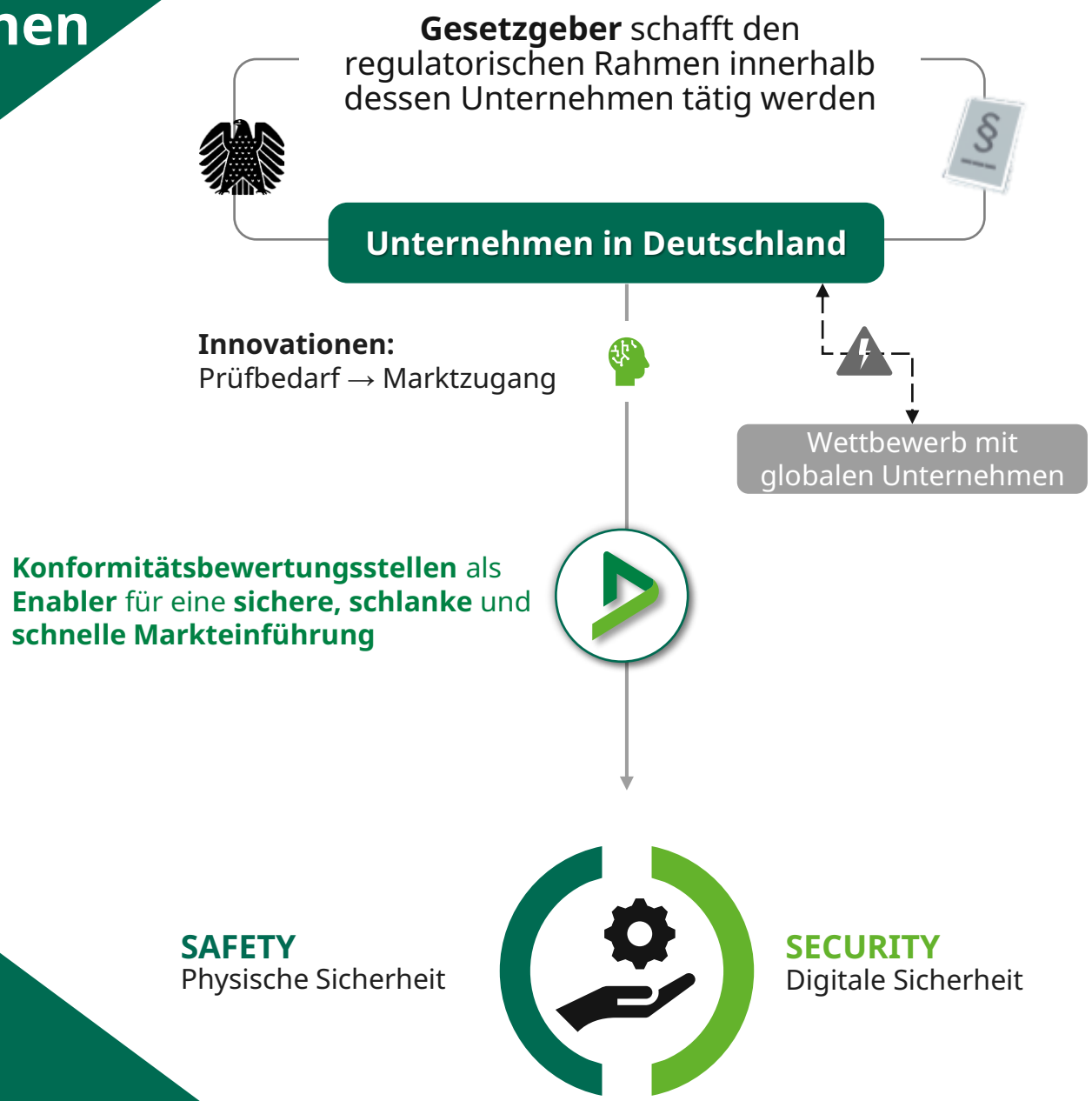
# IV. Vertrauen ermöglicht Innovationen

**Innovation braucht Vertrauen:** Das ist nur möglich, wenn sowohl die **physische Sicherheit (Safety)** als auch der **Schutz vor gezielten Cyberabgriffen (Security)** zuverlässig gewährleistet wird.

- **Technisches Vertrauen:** Produkte wie autonome Fahrzeuge oder Industrieanlagen sind sicher und manipulationsgeschützt.
- **Prozessuales Vertrauen:** Prüf- und Zertifizierungsverfahren folgen transparenten, anerkannten Standards.
- **Gesellschaftliches Vertrauen:** Menschen akzeptieren neue Technologien, weil sie zuverlässig und sicher sind.

Die **TIC-Branche** sorgt als **unabhängiger Partner** für **Sicherheit und Compliance** und ermöglicht so die nachhaltige Akzeptanz von Innovation.

**DEKRA** vereint im weltweit ersten „**Digital Trust“-Service** funktionale, digitale und KI-Sicherheit.



# V. KI im Gesundheitswesen: Brustkrebserkennung

## Warum ist es wichtig?

**Künstliche Intelligenz (KI)** kann Leben retten – beispielsweise durch eine frühzeitigere und genauere Diagnose von Brustkrebs. Fehler könnten jedoch schwerwiegende Folgen für die Patienten haben.

## Die Rolle von DEKRA

Wir tragen dazu bei, **Innovation und Sicherheit in Einklang** zu bringen, indem wir:

- Vertrauen durch unsere unabhängigen KI-Dienstleistungen aufbauen.
- Sicherer und verantwortungsvoller Zugang zum europäischen Markt ermöglichen.

## Ein aktuelles Beispiel

In den USA **wurde das erste KI-Tool zur Vorhersage des Brustkrebsrisikos** zugelassen. In Europa wird ein solches System als **Hochrisiko-KI-System** eingestuft – da es direkte Auswirkungen auf die Gesundheit und Sicherheit von Menschen hat.

## Was bedeutet das?

- Bevor diese Systeme auf den europäischen Markt kommen, müssen sie **strengen KI-Tests** unterzogen werden: von der Datenqualität und -sicherheit bis hin zur Zuverlässigkeit der Ergebnisse: Data Quality (ISO 5259) Model Accuracy & Robustness (ISO 24027/ ISO 24029) AI Security (OWASP)

# VI. DEKRA Prüfung von KI für Innovationen und Verbraucherschutz – at a glance

- **Ganzheitliche KI-Bewertung** über den gesamten Lebenszyklus: Entwicklung, Validierung, Betrieb
- **Audits & Risikoanalysen** zur Identifikation von Schwachstellen und Absicherung durch Risikobewertungspläne
- **Training:** Unternehmen „fit for KI“ machen und beim Aufbau von AI-Managementsystemen unterstützen
- **Regulatorische Expertise:** Begleitung bei Umsetzung kommender Vorschriften und Bewertung ihrer Auswirkungen
- **Prüfung & Zertifizierung:** Erste Generation umfassender Dienstleistungen zu KI-Lösungen

## SCHULUNG & VORBEWERTUNG

### KI-Schulung & Beratung

Schulungen und Vorbewertungsleistungen durch Experten zu verschiedenen Aspekten von KI-Technologie und Regulierung

- Bewusstsein für KI-Risiken
- KI-Regulierungen und Standards
- Vertrauenswürdigkeit und Ethik
- Bereitschaftsbewertung

## BEWERTUNG

### KI-Audit & Zertifizierung

Bewertung und Konformität in Bezug auf Standards und Best Practices für die Entwicklung und den Betrieb von KI-Lösungen

- Managementsystem (ISO 42001)
- KI-Risikomanagement (ISO 23894)
- Bewertung der Datenkennzeichnung (ISO 5259-4)
- Straßenfahrzeugsicherheit und KI (ISO 8800)
- A-SPICE Machine Learning

### KI-Prüfung

DEKRA KI-Experten führen umfassende Bewertungen mit modernsten Software-Tools durch

- Datenqualität (ISO 5259)
- Modellrobustheit (ISO 24029)
- KI-Bias & Fairness (ISO 24027)
- KI-Sicherheit

# VII. Rolle Gesetzgeber: Klarer gesetzlicher Rahmen für ein vertrauensbasiertes Level Playing Field

## Politischer Rahmen

Sowohl auf europäischer als auch auf nationaler Ebene rücken Cybersicherheit und digitale Souveränität immer mehr in den regulatorischen Fokus.

- **AI Act**
  Einbindung von unabhängigen Dritten insbesondere für Hochrisiko-KI-Systeme fest verankern, Typengenehmigung von Fahrzeugen (automatisierte Fahrzeuge als sicherheitsrelevant einstufen)
- **NIS-2 & KRITIS-Dachgesetz**
  Klassifizierung und Schutz kritischer Infrastrukturen, Prüforganisationen unterstützen Behörden und Unternehmen
- **Cyber Resilience Act**
  Sicherheitsanforderungen für digitale Produkte
- **Konformitätsbewertungspflichten** und die **Marktüberwachung** sichern die Umsetzung

Ziel ist einheitliche Standards & Normen zu schaffen, um so ein höchstmögliches Sicherheitsniveau für digitale Produkte & Infrastrukturen zu gewährleisten.

## Verantwortung der TIC-Branche

Unabhängige Prüforganisationen sind Teil der Lösung und tragen Verantwortung bei der Gestaltung und Umsetzung des regulatorischen Rahmens.

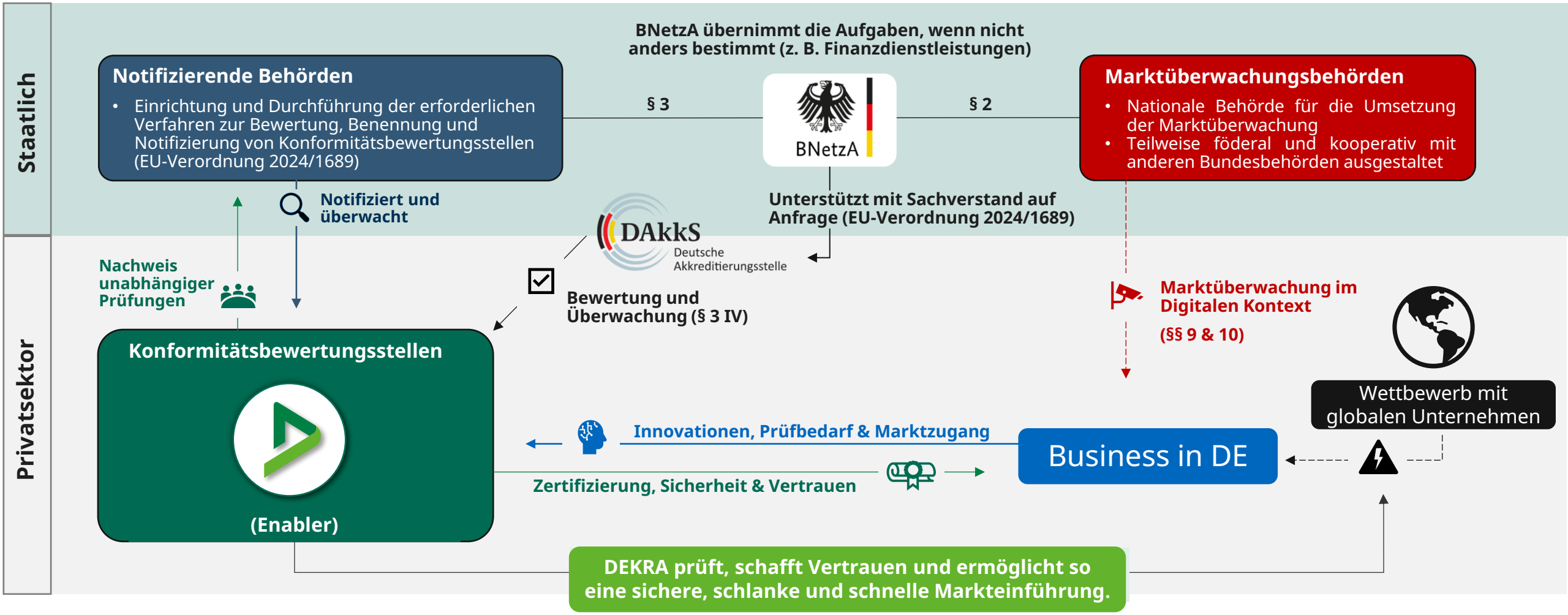
**Wesentliche Aufgaben dabei sind:**

- Durchführung unabhängiger Prüfungen
- Zertifizierungen und Audits zur Sicherstellung hoher Sicherheitsstandards
- Beratung von Herstellern und Betreibern bei der Umsetzung komplexer regulatorischer Anforderungen
- Aktive Einbindung in die Gestaltung von Normen und gesetzlichen Vorgaben durch den fachlichen Austausch mit politischen Entscheidungsträgern
- Unterstützung der Marktüberwachungsbehörden durch technische Expertise, um die Einhaltung der Vorschriften sicherzustellen


**Sicherheit** schafft **Vertrauen** – dafür braucht es einen klaren **gesetzlichen Rahmen**, **unabhängige Prüfungen** und starke **Standards**, die auch für den **Mittelstand** umsetzbar bleiben.

# VIII. Marktüberwachung im digitalen Kontext: AI Act

**Governance-Trias der Produktregulierung:** Unabhängige Prüforganisationen sind Teil der Lösung

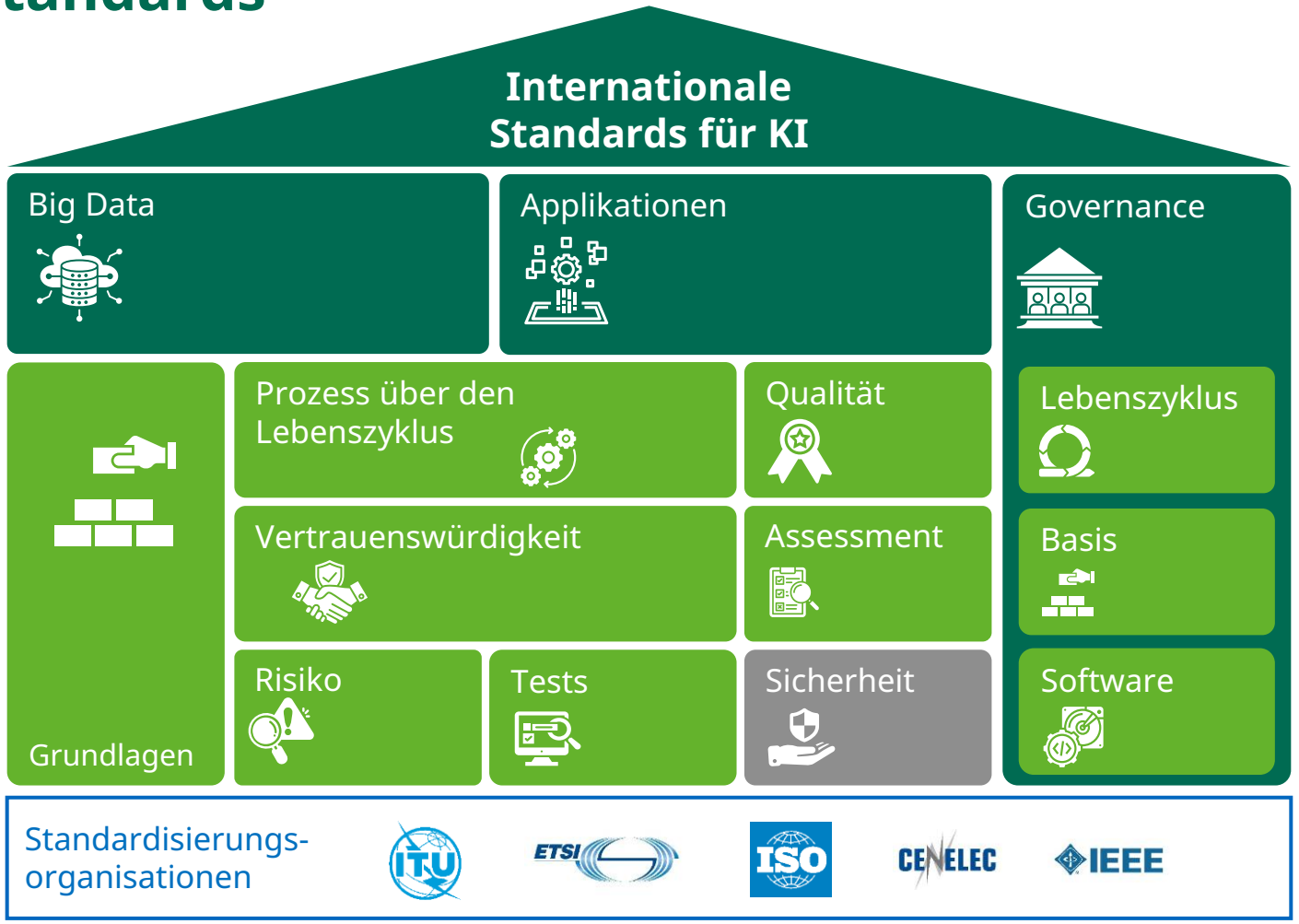



* Alle §§ beziehen sich auf den Referentenentwurf des Bundesministeriums für Digitales und Staatsmodernisierung des Gesetzes zur Durchführung der KI-Verordnung vom 04.08.2025.

# IX. Übersicht KI-relevante Standards

**Kompass zur Navigation wird benötigt**

- → Gesetzgebung, wie der EU AI Act, geht Hand in Hand mit der internationalen Entwicklung neuer Standards und Normen
- → Das Ziel besteht darin, etablierte Standards zu berücksichtigen und neue zu gestalten
- → Gemeinsame und harmonisierte Standards sind die unabdingbare Basis für ein innovatives und sicheres KI-Ökosystem




**37** **Entwickelte Standards**

**47** **Derzeit in Entwicklung**

# X. Fazit

Zentrale Rahmenbedingungen

## Zügige Umsetzung des EU AI Acts und NIS-2

- Zügige nationale Implementierung der europäischen Rahmenbedingungen für den sicheren und vertrauenswürdigen Einsatz digitaler Technologien
- Konformitätsbewertung durch TIC-Branche

## Globale Standards für KI & Cybersecurity

- Implementierung und globale Harmonisierung für ein sicheres und innovatives Ökosystem

## Förderung von Datensouveränität

- Nutzer sollten die Kontrolle über ihre Daten behalten
- Zugang für unabhängige Dritte auf unbearbeitete Sicherheits- & umweltrelevante Daten im Sinne des Verbraucherschutzes

## Unterstützung kleiner & mittlerer Unternehmen

- Gezielte Förderprogramme, Unterstützungsnetzwerke & Stärkung Digital Literacy
- Abbau bürokratischer Hürden

## Effektive Governance-Strukturen

- Klare Definition von zentralisierten Verantwortlichkeiten und Regeln sowie auskömmliche Ressourcen

## Investitionen in die digitale Infrastruktur

- Ausbau moderner, sicherer & leistungsfähiger digitaler Infrastrukturen als Fundament für innovative & resiliente digitale Ökosysteme

## Typengenehmigung von Fahrzeugen

- In Anbetracht von potenziellen Risiken von KI-Anwendungen bei AVs, sollten auch KI-Systeme als Sicherheitskomponenten eingestuft werden (UN-Regelungen Nr. 155 & 156)

100 YEARS
SECURING THE FUTURE
1925 – 2025

# Dr. Fabienne Beez

Leiterin Konzernrepräsentanz Berlin
DEKRA SE