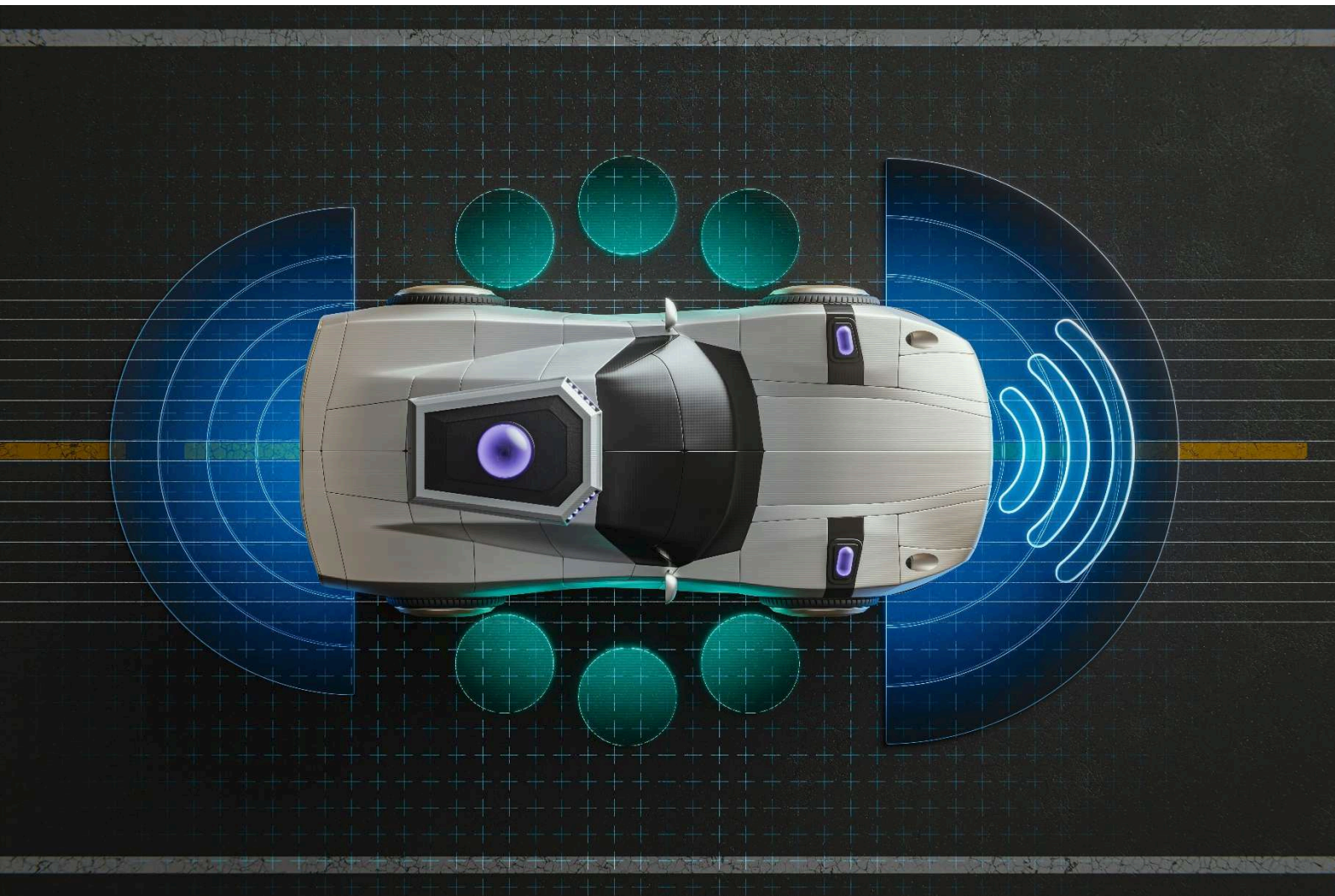
TÜV VERBAND

Berlin
Mai 2025

Grundpfeiler für eine moderne Mobilität

Digital Car – Sicherheit, effiziente Regulierung und unabhängige Prüfung



Inhaltsverzeichnis

Executive Summary

Der Automobilsektor befindet sich im Umbruch: Elektrifizierung, Vernetzung und Automatisierung verändern Mobilität grundlegend. Neben beträchlichen Chancen ergeben sich auch neue Herausforderungen – vor allem in den Bereichen Sicherheit, Regulierung und Cybersecurity. Das Positionspapier des TÜV-Verbands analysiert diese Entwicklungen und zeigt auf, wie unabhängige Prüfung, effiziente Regulierung und technische Innovation den Weg in die Zukunft ebnen können. Notwendig sind diese sieben Kernbereiche:

1. **Autonomes Fahren sicher einführen**
   Deutschland kann mit dem Gesetz zum autonomen Fahren und der Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (AFGBV) immer noch eine Vorreiterrolle bei der sicheren Zulassung von hoch- und vollautomatisiertem („autonomen") Fahrzeugen (SAE Level-4) einnehmen. Der Erfolg hängt jedoch von einer hohen Investitionsbereitschaft, praxisorientierten Genehmigungsverfahren und gesellschaftlicher Akzeptanz ab. Insbesondere Logistikanwendungen bieten zeitnah Chancen für den effizienten Einsatz autonomer Fahrzeuge. Die europäische Harmonisierung der bestehenden Regelwerke bleibt dabei essenziell.

2. **Künstliche Intelligenz zuverlässig integrieren**
   Um die gesellschaftlichen Vorteile autonomer Fahrzeuge zu gewährleisten, müssen Innovation und Regulierung sich auf vertrauensbildende Praktiken bei der Nutzung künstlicher Intelligenz konzentrieren, die Sicherheit, Transparenz und ethische Verantwortung einschließen. Sicherheitskritische KI-Systeme in Fahrzeugen bedürfen risikoadäquater Prüfung und zertifizierter Updates. Der TÜV-Verband fordert ein verpflichtendes unabhängiges Prüfungsschema im Third-Party-Prinzip, die Einführung eines europäischen „Datatrust" sowie effektive Testverfahren, um Datensicherheit und Zuverlässigkeit sicherzustellen.

3. **Digitale Fahrzeugakte (dFZA) einführen**
   Die digitale Fahrzeugakte enthält Informationen über technische Spezifikationen, Wartungshistorie, Reparaturen, Schadensfälle, und viele weitere Daten. Somit ermöglicht die dFZA eine sichere, transparente Dokumentation aller relevanten Informationen zum Fahrzeug während des Fahrzeuglebenszyklus. Voraussetzung sind einheitliche technische Standards und Schnittstellen, eine Anpassung der Rechtslage und ein zentrales europäisches Register.

4. **Datenzugang klar regeln**
   Der direkte Zugriff auf fahrzeuggenerierte Daten für unabhängiger Dritte zur Wahrnehmung hoheitlicher Aufgaben im Bereich von Verkehrssicherheit und Umweltschutz ist bisher unzureichend geregelt. Dieses Versäumnis gefährdet die Sicherheit und das Vetrauen in Innovationen. Der TÜV-Verband fordert verbindliche Standards für ein unabhängiges Datenmanagement,

gleichberechtigten Datentransfer und eine sektorspezifische Regulierung über den EU Data Act hinaus.

5. **Datenschutz bei der Genehmigung von Kraftfahrzeugen mit autonomen Fahrfunktionen**
   Die datenschutzkonforme Genehmigung von Fahrzeugen mit autonomen Fahrfunktionen erfordert eine Verzahnung technischer Maßnahmen und DSGVO-konformer Regelungen. Hersteller müssen sichere Schnittstellen, Datensparsamkeit, Anonymisierung und ein effektives Einwilligungsmanagement gewährleisten, um individuellen Datenschutz, technischen Fortschritt und innovative Nutzungsmöglichkeiten moderner und sicherer Mobilität zu vereinen.

6. **Regelmäßige technische Überwachung (Periodical Technical Inspection – PTI) modernisieren**
   Prüfverfahren im Rahmen der PTI müssen an moderne Fahrzeugtechnologien angepasst werden, um über den gesamten Lebenszyklus die sichere Nutzung von Elektromobilität, fortschrittlichen Assistenzsystemen und Software Updates zu gewährleisten. Ein herstellerunabhängiger Zugang zu relevanten Fahrzeugdaten ist dafür unerlässlich. Auch die Inhalte der Typgenehmigung für die spätere technische Überwachung im Lebenszyklus des Fahrzeugs müssen besser abgestimmt werden.

7. **Cybersecurity durchgehend gewährleisten**
   Cybersecurity ist Pflicht über den gesamten Fahrzeuglebenszyklus. Hersteller müssen bereits ein Cybersecurity-Managementsystem (CSMS) anwenden. Hier sind jedoch Hürden bei den einzelnen Typgenehmigungsbehörden festzustellen. Der EU Cyber Resilience Act stellt neue Anforderungen. Diese müssen harmonisiert und praxistauglich gestaltet werden.

Nur durch eine Kombination aus klaren gesetzlichen Vorgaben, unabhängiger Prüfung und europäischer Harmonisierung lässt sich der Wandel zur digitalen, sicheren Mobilität erfolgreich gestalten. Der TÜV-Verband steht dabei als zuverlässiger Partner für Sicherheit, Innovation und Vertrauen bereit.

Einleitung

Der Automobilsektor steht an einem entscheidenden Wendepunkt. Klimawandel, Sicherheitsfragen im Zusammenhang mit Künstlicher Intelligenz (KI) und die steigende Nachfrage nach nachhaltigen Mobilitätslösungen sind dabei zentrale Treiber dieses tiefgreifenden gesellschaftlichen Wandels. Der Automobilsektor muss sich diesen vielfältigen Herausforderungen des Übergangs zur elektrifizierten, automatisierten und vernetzten Mobilität stellen.

Während der technologische Fortschritt die Grenzen dessen erweitert, was Fahrzeuge leisten können, rücken Sicherheit, regulatorische Konformität und gesellschaftliche Akzeptanz der Innovationen in den Fokus. Vor allem der Übergang zu SAE-Level-3- und Level-4-Systemen – also hoch- und vollautomatisiertem Fahren – verändert grundlegende Muster bei der Verantwortung und Haftung im Straßenverkehr. Als internattioanler Vorreiter hat Deutschland mit der Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (AFGBV) regulatorische Rahmenbedingungen geschaffen, die Fahrzeugtypgenehmigungen und Betriebsbereichsgenehmigungen klar definieren. Die aktuellen Erfahrungen aus zahlreichen Erprobungsgenehmigungen helfen technische Herausforderungen frühzeitig zu erkennen, rechtliche Rahmenbedingungen anzupassen und gesellschaftliche Akzeptanz zu fördern. Insgesamt zeigt sich international ein sehr unterschiedlicher Umgang mit autonomen Fahrzeugen: Während die USA auf schnelle Skalierung und marktgetriebene Entwicklung mit gigantischen Investitionssummen setzen, fokussiert sich China auf staatlich gesteuerte Innovation und Infrastrukturintegration.

Mit zunehmender Vernetzung und softwaregesteuerten Fahrzeugfunktionen nehmen potenzielle Cyberrisiken exponentiell zu und die Bedeutung von Cybersecurity wächst. Eine robuste und zertifizierte Cybersecurity wird zu einer entscheidenden Voraussetzung für die Akzeptanz und den Erfolg neuer Technologien. Auch die Herausforderung, KI-gesteuerte Fahrzeuge sicher und verantwortungsvoll in den Straßenverkehr zu integrieren, verlangt nach sorgfältiger Regulierung und kontinuierlicher Überwachung.

In diesem spannenden, aber komplexen Spannungsfeld kommt es maßgeblich auf unabhängige und neutrale Dritte an, die häufig hoheitliche Aufgaben im Zusammenhang mit Verkehrssicherheit und Umweltschutz wahrnehmen. Die TÜV-Unternehmen spielen als unabhängige Prüf-, Inspektions- und Zertifizierungsorganisationen (TIC) eine entscheidende Rolle bei der Digitalisierung und Automatisierung der Mobilität. Ihre Expertise garantiert, dass Innovationen den regulatorischen Anforderungen entsprechen und sowohl den Sicherheitsstandards als auch ethischen und ökologischen Erwartungen gerecht werden. Besonders bei hochautomatisierten Systemen stellt sich die Frage der Haftung neu, da hier KI-Systeme schrittweise menschliche Aufgaben übernehmen. Ein ausgewogener Regulierungsrahmen, der sowohl die Innovationsfähigkeit der Industrie unterstützt als auch öffentliche Sicherheitsinteressen schützt, ist deshalb unverzichtbar.

In diesem Positionspapier zeigt der TÜV-Verband auf, wie effiziente Regulierung, Sicherheit und unabhängige Prüfung nicht nur die Grundpfeiler für die Zukunftsfähigkeit des Automobilsektors sind. Sie sind auch entscheidend, um das Vertrauen der Öffentlichkeit in automatisierte und vernetzte Fahrzeuge nachhaltig zu stärken. Effiziente Regulierung bedeutet keineswegs mehr Bürokratie – im Gegenteil: Sie kann Bürokratie intelligent strukturieren und zielgerichtet einsetzen. Bürokratische Verfahren haben in vielen Bereichen einen unschätzbaren Wert: Sie gewährleisten Transparenz, Sicherheit und Gleichbehandlung. Besonders bei der Einführung automatisierter und vernetzter Fahrzeuge braucht es verlässliche, nachvollziehbare Standards. Bürokratieabbau darf daher nicht pauschal gefordert werden – gefragt ist vielmehr eine moderne, digital unterstützte Verwaltung, die überflüssige Prozesse reduziert, ohne zentrale Kontrollmechanismen auszuhöhlen. Der TÜV-Verband setzt sich deshalb für eine ausgewogene Balance ein: weniger lähmende Papierpflichten, aber klare Regeln und dokumentierte Verfahren zum Schutz von Menschen, Umwelt und Technik.

Autonomes Fahren auf Level 4: Empfehlungen für eine sichere und erfolgreiche Einführung

Die AFGBV ermöglicht es dem Kraftfahrt-Bundesamt (KBA), nationale Betriebserlaubnisse für Level-4-Fahrzeuge zu erteilen. Der Genehmigungsprozess umfasst zum einen die Fahrzeugtypgenehmigung und im Gegensatz zu herkömmlichen Fahrzeugen zusätzlich die Betriebsbereichsgenehmigung. Dabei beantragen die Hersteller zunächst eine Fahrzeugtypgenehmigung beim KBA, die durch einen Technischen Dienst geprüft wird. Anschließend erfolgt auf Antragstellung des Halters die Genehmigung des Betriebsbereichs durch die zuständige Landesbehörde oder die Autobahn GmbH.

Bisher liegen in Deutschland keine Anträge für den Regelbetrieb von Level-4-Fahrzeugen vor, allerdings wurden zahlreiche Erprobungsgenehmigungen erteilt. Die Erfahrungen aus Projekten auf Basis von Erprobungsgenehmigungen sind von zentraler Bedeutung. Sie helfen technische Herausforderungen frühzeitig zu erkennen, rechtliche Rahmenbedingungen anzupassen und gesellschaftliche Akzeptanz zu fördern. Durch ein strukturiertes Vorgehen, dass Erfahrungen direkt berücksichtigt, kann der Regelbetrieb autonomer Fahrzeuge effizient und nachhaltig etabliert werden.

Der EU-Gesetzgeber hat durch die in der Verordnung zur „Allgemeinen Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern" (GSRII – VO (EU) 2019/2144) und der Durchführungsverordnung 2022/1426 (Typgenehmigung des automatisierten Fahrsystems vollautomatisierter Fahrzeuge) eine vergleichbare Regulatorik geschaffen, so dass es in Europa grundsätzlich möglich ist, Fahrzeuge mit autonomer Fahrfunktion in Verkehr zu bringen. Auch die EU Gesetzgebung sieht sowohl die Genehmigung des Fahrzeuges und als auch die Genehmigung des Bereichs in dem dieses Fahrzeuges betrieben werden soll vor.

Im internationalen Vergleich zeigt sich, dass die Regulierung autonomer Fahrzeuge in den USA und Asien unterschiedlich gehandhabt wird:

- Die US-amerikanische Regulierung setzt, wie auch die europäische, auf eine schrittweise Einführung autonomer Fahrzeugtechnik und beginnen mit vorgegebenen Strecken oder Gebieten. Allerdings wird in den USA die Einführung autonomer Fahrzeuge von ein bis zwei Unternehmen mit gigantischer finanzieller Potenz dominiert. Der Ansatz ist stark marktorientiert, mit einem Fokus auf schnelle Erprobung und Skalierung in Großstädten. Die Technologien umfassen hauptsächlich Robotaxis und autonome Fahrzeugflotten, die stark auf KI-gestützte Sensorsysteme wie Kameras, Lidar und Radar setzen. Die Regulierung ist in den USA flexibler gestaltet. Die einzelnen Bundesstaaten regeln individuell und gewähren teilweise Freiheiten für Testgebiete, wie z.B. Kalifornien, Arizona und Nevada. Dieser Ansatz ermöglicht eine dynamische Weiterentwicklung der autonomen Fahrfunktionen und bietet Wettbewerbsvorteile durch die Größe des Marktes und hohe Investitionen in KI. Allerdings gibt es Sicherheitsprobleme, insbesondere bei unvorhergesehenen Verkehrssituationen, außerdem fehlen einheitliche Standards und die Nachvollziehbarkeit bei Entscheidungsalgorithmen.
- In China wird die Entwicklung von Level-4 Fahrzeugen stark staatlich gefördert und gelenkt. Ein hoher Fokus liegt auf urbanen Anwendungen und umfassender Datenintegration. Die Technologien sind ähnlich wie in den USA, jedoch mit einer breiteren Integration staatlicher Infrastruktur wie hochpräzisen Karten und einheitlichen Datennetzen (5G, Sensoren). Die Regulierung ist stark standardisiert und zentral kontrolliert, unterstützt durch staatliche Förderprogramme für Technologien wie KI und 5G sowie die Förderung von Testgebieten in Städten wie Beijing und Shanghai. Dies führt zu einer guten Infrastruktur für einheitliche und umfassende Datennutzung und schnellem Fortschritt durch staatliche Unterstützung und klare Richtlinien. Allerdings gibt es Bedenken bezüglich Datenschutz und ethischer Standards sowie oft weniger Innovationsspielraum durch staatliche Kontrolle.

Herausforderungen

Wenn es um komplexe Verkehrssituationen geht, stoßen hochautomatisierte Fahrfunktionen derzeit weltweit noch an Grenzen. Problematisch sind unter anderem Auffahrten auf die Autobahn, Tunnel, unübersichtliche Kreuzungen, schwierige Wetterbedingungen, veränderte Verkehrszeichen oder Störungen bei der Übertragung von GPS-Signalen. Die Übertragung der Fahraufgabe vom Menschen auf das Fahrzeug stellt alle Beteiligten vor große Herausforderungen.

Neben den technischen und rechtlichen Anforderungen ist die Ausarbeitung und Investitionsbereitschaft in tragfähige Geschäftsmodelle ein zentraler Faktor für den Erfolg autonomer Fahrzeuge im Regelbetrieb. Viele Erprobungen zeigen, dass ein reines Testumfeld zwar wichtige Erkenntnisse liefert, sich daraus aber nicht automatisch ein wirtschaftliches Betreiberkonzept ableiten lässt.

Ein prominentes Einsatzfeld für L4-Fahrzeuge ist der öffentliche Personennahverkehr. Doch dieser Bereich ist mit zahlreichen zusätzlichen Herausforderungen wie Tarifintegration, Leitstellenkonzepten und Kundenkommunikation verbunden. In anderen Anwendungsfelder – insbesondere in der Logistik – wären autonome Technologien schneller und effizienter realisierbar. Hier ist ein zentraler Ansatzpunkt die Off-Road-Güterbewegung. In klar abgegrenzten Umgebungen wie Flughäfen, Minen, Logistikzentren oder Fabriken können autonome Fahrzeuge bereits heute zum Einsatz kommen. Diese Umgebungen bieten kontrollierte Bedingungen und etablierte Sicherheitsstandards, die die Einführung automatisierter Transportsysteme deutlich erleichtern. Ein weiterer pragmatischer Schritt wäre die Nutzung autonomer Fahrzeuge für Hub-to-Hub-Transporte. Auf festen Routen zwischen Logistikzentren könnten autonome Fahrzeuge automatisiert eingesetzt werden. Diese vordefinierten Strecken minimieren das Risiko unvorhersehbarer Verkehrssituationen und ermöglichen eine schrittweise Integration autonomer Systeme in den Güterverkehr. In diesem Kontext wurde in Europa bereits das Platooning, also das Fahren mehrerer Lkw mit in Kolonne geringem Abstand, erfolgreich getestet. Im Hub-to-Hub-Betrieb könnte dieses Konzept auf zwei gekoppelte Lkw-Züge übertragen werden, wobei der zweite Lkw-Zug teilautonom und fahrerlos geführt wird. Da die breite Einführung autonomer Fahrzeuge stark von der Akzeptanz in der Bevölkerung abhängt, würden schnell realisierbare Projekte die Sichtbarkeit erhöhen und zu mehr Vertrauen in die Nutzung autonomer Fahrzeuge beitragen.

Um einen sicheren und reibungslosen Verkehrsfluss herzustellen, bedarf es weiterer Forschung und technischer Unterstützung (Standardisierung und Regulierung) dess Zusammenwirkens von L-4-Fahrzeugen mit der herkömmlichen Fahrzeugflotte und/oder anderen Verkehrsteilnehmer:innen sowie mit der Straßeninfrastruktur (V2V, V2I, I2V-Kommunikation). Für einen sicheren Regelbetrieb autonomer Fahrzeuge ist eine leistungsfähige digitale Infrastruktur unerlässlich. Dazu gehören breitbandige Mobilfunknetze – idealerweise 5G – und auch WiFi-Technologie, die eine zuverlässige Kommunikation zwischen Fahrzeug und Leitstelle ermöglichen. Ebenso spielt die Straßeninfrastruktur eine zentrale Rolle: Klare Markierungen, gut sichtbare Beschilderungen und gegebenenfalls zusätzliche Sensorik in Form von C-ITS-Systemen tragen zur sicheren Navigation bei. Ein weiterer wichtiger Baustein sind standardisierte Datenschnittstellen und hochpräzise Kartendienste. Sie stellen den Fahrzeugen detaillierte und stets aktuelle Informationen über ihre Umgebung zur Verfügung und verbessern so die maschinelle Entscheidungsfindung während der Fahrt. Besonders entscheidend ist das reibungslose Zusammenspiel zwischen Fahrzeug, Technischer Aufsicht (Leitstelle) und Verkehrsumgebung. Nur durch eine umfassende Vernetzung aller Komponenten können Sicherheit und Effizienz im autonomen Straßenverkehr gewährleistet werden.

Handlungsempfehlungen

- Schaffung von Routine und Transparenz in Genehmigungsprozessen: Der bestehende Rechtsrahmen in Deutschland und auf EU-Ebene setzt wesentliche Standards. Sowohl Hersteller und Betreiber als auch Genehmigungsbehörden und Technische Dienste bewegen sich bei der Anwendung des Rechtsrahmens bisher jedoch noch auf unbekanntem Terrain. Dieses Terrain gilt es gemeinsam so zu gestalten, dass der Regelbetrieb für Level-4-Fahrzeuge, z. B. das Platooning im autonomen Hub-to-Hub-Verkehr, in absehbarer Zukunft zur Normalität wird. Die Genehmigungsprozesse könnten zudem in Simulationsprojekten nach dem Sand-Box-Ansatz weiter erprobt werden, um mehr Routine und Normalität in der Anwendung zu schaffen und darauf aufbauend auch mögliche Anpassungen der Regulatorik im Sinne einer einheitlichen und effizienten Umsetzung ableiten zu können. Es bedarf einer engen und regelmäßigen Abstimmung aller Beteiligten. Daher sollten die Arbeiten am Thema Autonomes Fahren durch den Verordnungsgeber gebündelt und vereinfacht werden, beispielsweise durch die geplante Einrichtung eines bundesweiten Fachausschusses Autonomes Fahren nach Vorbild der Bund/Länder-Fachausschüsse.

- Aufbau von Szenariendatenbanken unter Beteiligung der TÜV-Organisationen: Für die sichere Genehmigung und spätere technische periodische Untersuchung (HU) automatisierter und autonomer Fahrzeuge wird die Nutzung von Testszenarien im Rahmen von Simulation und Realtests immer wichtiger. TÜV-Organisationen übernehmen dabei eine aktive Rolle bei der Erstellung, Pflege und Zertifizierung von standardisierten Szenarien und entsprechender Datenbanken. Diese Datenbanken können nicht nur im Genehmigungsprozesss von Level-4- und Level-5-Fahrzeugen genutzt weden, sondern auch im Rahmen der HU der Fahrzeuge eine zentrale Rolle spielen.

- Europäische Harmonisierung und Beteiligung der TÜV-Organisationen an „Automated Driving Corridors“: Dringend notwendig für den europäischen Standort bleibt die Harmonisierung der gesetzlichen Rahmenbedingungen zwischen den europäischen Mitgliedstaaten. Die aktuell fragmentierte Regulierung erschwert die Einführung autonomer Fahrzeuge erheblich. Eine einheitliche Gesetzgebung mit standardisierten Genehmigungsverfahren im gesamten Binnenmarkt für die Genehmigung von Level-4 Fahrzeugen ist essenziell, um Innovationen effizient voranzutreiben, doppelte Regulierungsverfahren zu vermeiden und vor allem grenzüberschreitende Mobilität zu ermöglichen. Die EU-Kommission setzt mit ihrem „Industrial Action Plan for the European automotive sector“ (COM(2025) 95) entscheidende Impulse für die Zukunft des autonomen Fahrens. Besonders hervorzuheben sind die geplanten grenzüberschreitenden Testumgebungen, die es ermöglichen, autonome Fahrzeuge unter realen Bedingungen zu erproben. Die Einrichtung von drei großen Autonomous Driving Corridors wird dazu beitragen, technologische Entwicklungen praxisnah zu evaluieren und die Markteinführung innovativer Systeme zu beschleunigen. TÜV-Organisationen können sich hier frühzeitig als

Evaluierungs- und Zertifizierungspartner einbringen. Aufgrund ihrer umfangreicher Erfahrung bei der Evaluierung von Infrastrukturprojekten im Verkehrsbereich allgemein sowie spezifisch in Bezug auf die Begutachtung von Betriebsbereichen autonomer Fahrzeuge sind die TÜV-Unternehmen in der Lage die Bewertung und Qualitätssicherung der Infrastruktur entlang dieser Korridore zu übernehmen. Die aktive Mitwirkung der TÜV-Organisationen an der Skalierung und Harmonisierung der Infrastrukturanforderungen entlang dieser Testkorridore wäre ein entscheidender Beitrag zur europäischen Standardisierung und zur Beschleunigung der Markteinführung autonomer Systeme.

- Cybersicherheit und Datenschutz stärken: Die steigende Vernetzung autonomer Fahrzeuge erzeugt eine Vielzahl an sensiblen Daten. Sowohl personenbezogene Daten (Fahrgastinfos) als auch Fahrzeug- und Umfelddaten (Standort, Fahrprofile) sind zu schützen. Gleichzeitig gewinnen Cybersicherheitsfragen an Bedeutung: Angriffe auf Fahrzeuge, Leitstellen oder Datenleitungen könnten zu erheblichen Gefahren im Straßenverkehr führen. Daher sind umfassende IT-Sicherheits- und Datenschutzkonzepte für einen sicheren Regelbetrieb unverzichtbar.
- Fokus auf Logistik: Statt sich vordergründig auf autonome Lösungen im ÖPNV zu konzentrieren, sollten politische Entscheidungsträger:innen und Unternehmen verstärkt die Potenziale im Logistiksektor in den Blick nehmen. Hier könnten kurzfristig technologische Fortschritte effizient genutzt werden, um Verkehrsströme zu entlasten und die Effizienz der Transportketten erheblich zu steigern.

Sicherheitskritische, lernende KI-Systeme im Automobilsektor

Künstliche Intelligenz (KI) spielt bereits heute eine zentrale Rolle in modernen Fahrzeugen und wird für die Zukunft vernetzter und automatisierter Fahrzeuge weiterhin zentraler Treiber sein. Dabei ist KI nicht gleich KI: neben klassischen mit maschinellen Lernverfahren (ML) entwickelten Systemen erhalten zunehmend auch generative KI-Lösungen und Schnittstellen Einzug in die Fahrzeuge und Mobilität. Mit der fortschreitenden Automatisierung gewinnen sicherheitskritische, lernende KI-Systeme an Bedeutung, insbesondere in hochautomatisierten Fahrfunktionen.

Ein von der UNECE veröffentlichtes Dokument mit Erwägungen zu KI im Automobilbereich beschreibt KI als ein durch maschinelles Lernen und neuronale Netze trainiertes System, das sowohl regulatorische als auch technische Herausforderungen mit sich bringt (Considerations on Artificial Intelligence in the context of road vehicles (WP.29-193-20). Auch wenn der Einsatz von sicherheitskritischen Anwendungen, die im Realeinsatz kontinuierlich lernen derzeit regulatorisch ausgeschlossen ist, können prinzipiell Modellupdates auf Basis der Anwendung von Lernverfahren außerhalb des Betriebs erfolgen, was zusätzliche Anforderungen an Genehmigung, Prüfprozesse und Langzeitüberwachung zur Folge haben kann.

Der EU AI Act (EU VO 2024/1689) klassifiziert sicherheitskritische Fahrfunktionen als Hochrisiko-KI. Daraus ergeben sich strenge Sicherheits- und Zuverlässigkeitsstandards sowie regulierte Zertifizierungs- und Auditprozesse über den gesamten Lebenszyklus. Diese sind voraussichtlich ab dem Jahr 2027 in die Fahrzeugtypgenehmigung nach VO (EU) 2018/858, VO (EU) 167/2013, VO (EU) 168/2013 sowie GSR2 (VO (EU) 2019/2144) einzubinden.

Die zentrale Schwierigkeit liegt in der Natur der KI-Systeme: Sie verändern sich im Laufe der Zeit – und damit ergeben sich neue Chancen und Herausforderungen für die künftige Automobilität, insbesondere in der Phase nach der erstmaligen Zulassung. Während klassische Fahrzeugsysteme über Jahre hinweg stabil bleiben, müssen bei Updates sicherheitskritischer, lernenden KI-Systeme folgende Herausforderungen beachtet werden:

- Kontinuierliche Anpassung der Modelle durch erneutes Training zur Berücksichtigung neuer Verkehrsszenarien
- Nachvollziehbarkeit und Transparenz (Überprüfbarkeit) von KI-Entscheidungen zur Minimierung von Fehlerquellen
- Validierung von Trainingsdaten durch neutrale Dritte statt ausschließlich KI-gestützter Filterung und Klassifikation (Datenqualität und -neutralität)
- Schließung von Regulierungslücken bei Fahrzeugtypgenehmigung und Zertifizierung, um auch nach Updates hohe Sicherheitsstandards zu gewährleisten (Stabilität im Fahrzeuglebenszyklus)

Zentrale Bedeutung nimmt zusätzlich das Thema KI-Sicherheit ein. Die Systeme müssen in der Lage sein, zusätzlichen Herausforderungen zu begegnen, die über die klassischen Aspekte der IT-Sicherheit hinausgehen. So müssen KI-Systeme z.B. lernen, anhand von Kontextinformationen mit projizierten oder manipulierten Verkehrsschildern umzugehen.

Harmonisierung von KI-Definitionen und Klassifizierungen

Hochrisiko-KI-Systeme, die als sicherheitskritische Bauteile gelten, müssen in der Fahrzeugtypgenehmigung eindeutig definiert und reguliert werden. Dabei sollten die Begriffe aus der UNECE-Resolution, wie Modelldrift, Verifizierbarkeit, Robustheit und Vorhersagbarkeit, berücksichtigt werden. Zudem ist eine klare Unterscheidung zwischen symbolischer KI (regelbasiert, deterministisch) und verbindungsbasierter KI (maschinelles Lernen, neuronale Netze) erforderlich, da letztere besondere Prüf- und Sicherheitsmechanismen erfordert. Lernende KI-Systeme sollten nur unter strengen Bedingungen erlaubt sein und keine sicherheitskritischen Fahrfunktionen beeinflussen, solange keine Prüfung und Zertifizierung zur Freigabe der neuen/erweiterten Funktionen erfolgt ist.

Einführung von Prüf- und Genehmigungsprozessen

Ein umfassendes unabhängiges Genehmigungsmodell für sicherheitskritische, lernende KI muss implementiert werden. Vor dem Inverkehrbringen einer KI-gestützten Fahrfunktion ist eine Prüfung durch eine unabhängige Sachverständigenorganisation erforderlich, die sich insbesondere auf folgende Punkte konzentriert:

- Erklärbarkeit der KI-Entscheidungen (Explainable AI, XAI) für eine erfolgreiche Markteinführung und Kundenakzeptanz
- Stabilität der Modelle und Sicherheit bei der Installation der neuesten Updates
- Integration von Modelldrift-Kontrollen zur Vermeidung unbemerkter Leistungsverschlechterungen

Zudem sind unabhängige Prüfungen der Modellupdates erforderlich, bevor diese in den Live-Betrieb übergehen. Neben der Erstgenehmigung sollte ein verpflichtendes „Änderungs-Genehmigungs-Verfahren" für sicherheitskritische KI-Updates eingeführt werden. Auch zyklische Prüfungen im Fahrzeuglebenszyklus, etwa durch Integration in die Hauptuntersuchung (HU) oder spezielle KI-Inspektionen, sind erforderlich. Harmonisierte Testmethoden sollten an bestehenden Standards ausgerichtet werden, darunter ISO 26262 (funktionale Sicherheit), ISO 21434 (Cybersecurity), ISO/TR 4804 (szenarienbasiertes Testen) und UNECE NATM (New Assessment/Test Method for Automated Driving).

Sicherstellung der Datenqualität und Datenneutralität

Die Qualität der Trainingsdaten hat direkte Auswirkungen auf die Sicherheit von KI-Systemen. Daher ist es notwendig, eine unabhängige Datenprüfung und -verwaltung einzuführen. Um Verzerrungen in KI-Modellen zu vermeiden, sollte ein „European Datatrust" als unabhängiges Datentreuhändermodell eingeführt werden. Trainings- und Testdaten müssen aus realen Fahrsituationen gewonnen werden, um zu verhindern, dass Fehler aus KI-generierten Daten durch die KI weitergegeben werden. Sie müssen durch neutrale Stellen geprüft werden, um sicherzustellen, dass Trainingsdaten nicht ausschließlich von KI-Systemen gefiltert und klassifiziert werden. Datensätze müssen repräsentativ und divers sein, um unfaire oder diskriminierende KI-Entscheidungen (Modellbias bzw. Modellverzerrungen) zu verhindern.

Einführung von Simulations- und Testverfahren

Sicherheitskritische KI muss vor ihrer Implementierung in Fahrzeugen umfassend in Simulationsumgebungen und unter Realbedingungen validiert werden. Eine EU-weite Szenariendatenbank für sicherheitskritische Tests sollte aufgebaut werden.

Für lernende KI-Modelle sollte ein „Shadow Mode"-Testing Standard werden. Hierbei können Algorithmen

neue Szenarien trainieren, ohne aktiv ins Fahrverhalten einzugreifen. Dadurch lassen sich potenzielle Risiken identifizieren, bevor eine reale Implementierung erfolgt. Im Rahmen einer „Änderungs-Genehmigungs-Verfahren" beispielsweise im Rahmen einer Erweiterung der Typgenehmigung können neue verbesserte Updates zugelassen werden, insofern diese neuen Funktionen etwa von Assistenzsystemen aus sicherheitstechnischer Sicht zuverlässig ergänzen können.

Fazit und Empfehlungen

Vertrauenswürdige Methoden im Umgang mit künstlicher Intelligenz – etwa in Bezug auf Sicherheit, Transparenz und ethische Verantwortung – müssen im Zentrum von Innovation und Regulierung stehen, um die gesellschaftlichen Vorteile autonomer Fahrzeuge zu gewährleisten. KI-Systeme müssen unter allen Bedingungen zuverlässig funktionieren – selbst in unerwarteten Situationen oder extremen Wetterlagen. Dabei spielt besonders die Absicherung gegen Cyberangriffe eine zentrale Rolle, um Manipulationen zu verhindern. Die Validierung und Verifizierung solcher Systeme, vorallem wenn sie lernende Algorithmen nutzen, sind äußerst komplex und erfordern neue Methoden und Ansätze. Hinzu kommt der Aspekt von Datensicherheit und Datenschutz. Da KI-Anwendungen große Datenmengen zum Lernen benötigen, ist der Schutz dieser Daten vor unbefugtem Zugriff unverzichtbar. Auch die Privatsphäre der Nutzer:innen muss gewahrt bleiben – insbesondere, wenn personenbezogene Daten erfasst und verarbeitet werden.

Schließlich ist auch die gesellschaftliche Dimension von großer Bedeutung. Akzeptanz von und Vertrauen in KI-gesteuerte Fahrzeuge entstehen nur, wenn die Gesellschaft von deren Sicherheit und Zuverlässigkeit überzeugt ist. Aufklärung, Transparenz und unabhängige Drittprüfungen sind wesentlich, um Ängste und Vorbehalte abzubauen. Gleichzeitig können sie die Marktdurchdringung innovativer, KI-gestützter Mobilitätslösungen beschleunigen.

Die sichere Integration von KI im Fahrzeugsektor erfordert eine Kombination aus klaren Regulierungen, unabhängiger Prüfung und harmonisierten Testverfahren. Folgende Maßnahmen für eine sichere und transparente Einführung von KI im Straßenverkehr müssen hierfür zusammenfassende ergriffen werden:

- Einheitliche Definitionen und klarer Rechtsrahmen für sicherheitskritische, lernende KI im Einklang mit der UNECE-Perspektive und dem EU AI Act
- Verpflichtende Zertifizierungs- und periodische Änderungs-Genehmigungs-Verfahren für alle sicherheitskritischen KI-Modelle
- Aufbau einer europäischen Infrastruktur für KI-Daten und Simulationen zur Validierung und Testung unabhängig von Herstelllern
- Integration von KI-Prüfungen in bestehende Verfahren der Fahrzeugtypgenehmigung und Hauptuntersuchung

Die digitale Fahrzeugakte und ihr Potenzial für sichere Software Updates und vernetzte Mobilität

Die Einführung einer digitalen Fahrzeugakte (dFZA) ist ein essenzieller Schritt zur Modernisierung des Fahrzeugmanagements. Sie ermöglicht eine umfassende, transparente und manipulationssichere Dokumentation aller relevanten Fahrzeugdaten über den gesamten Lebenszyklus hinweg. Dies bringt erhebliche Vorteile für Fahrzeughalter:innen, Behörden, Prüfstellen sowie auch die Automobil- und Versicherungsbranche. Fahrzeughalter:innen profitieren davon, dass alle relevanten Informationen – von Wartungsarbeiten über Rückrufe bis hin zu sicherheitsrelevanten Software-Updates – digital verfügbar sind. Die physische Dokumentenverwaltung entfällt, während gleichzeitig die Transparenz über den technischen Zustand des Fahrzeugs steigt. Verbraucher:innen erhalten eine verlässliche und jederzeit abrufbare Fahrzeughistorie, was Manipulationen – etwa am Kilometerstand – erschwert und den Gebrauchtwagenmarkt sicherer macht. Auch für Versicherungen und Steuerbehörden bietet die dFZA Vorteile, da fahrzeugbezogene Beiträge verursachergerecht berechnet werden können, insbesondere bei temporären Leistungssteigerungen oder Zusatzfunktionen.

Für Behörden und Prüfstellen erleichtert die digitale Fahrzeugakte die Überprüfung und Feststellung der Vorschriftsmäßigkeit eines Fahrzeugs, sowohl bei Hauptuntersuchungen (HU) als auch bei Polizeikontrollen. Der Zulassungsprozess kann durch die digitale Übermittlung von Daten effizienter gestaltet werden. Besonders für moderne, softwaredefinierte Fahrzeuge (Software-Defined Vehicles) ist die digitale Erfassung essenziell, da Software-Updates und Automatisierungsgrade jederzeit nachvollziehbar sein müssen. Denn Software-Updates müssen immer in Bezug auf das jeweilige Fahrzeug vorgenommen werden, wobei der bauliche Zustand, die Konfiguration und die vorgenommenen Änderungen zu berücksichtigen sind. Aus Sicht des Herstellers wäre es fatal seinen Kunden eine Software-Update anzubieten, das auf der Fahrzeug-Hardware nicht funktioniert.

Herausforderungen bei der Umsetzung und notwendige Maßnahmen

Trotz der offensichtlichen Vorteile stellen sich mehrere Herausforderungen, die eine gezielte regulatorische und technische Weiterentwicklung erfordern. Eine zentrale Schwierigkeit besteht darin, bestehende Datenbanken der unterschiedlichen Stakeholder miteinander zu verknüpfen. Ein standardisierter, sicherer und schneller Datenaustausch zwischen Herstellern, Zulassungsbehörden, Prüfinstitutionen und Halter:innen ist entscheidend für den Erfolg der dFZA.

Auf nationaler Ebene müssen bestehende rechtliche Rahmenbedingungen angepasst werden, um die digitale Erfassung und Verwaltung von Fahrzeugdaten zu ermöglichen. Dies betrifft insbesondere das Zulassungsrecht sowie die Vorschriften für technische Überwachung in der StVZO. Entsprechende rechtliche Initiativen wurden hierzu vom Gesetzgeber – entsprechend der finanziellen Möglichkeiten - bereits in Angriff genommen. Gleichzeitig muss sichergestellt werden, dass die technische Infrastruktur

den Anforderungen der Datenschutz-Grundverordnung (DSGVO) genügt.

Auf europäischer Ebene besteht eine noch größere Herausforderung: Die Vorschriften zur Fahrzeugzulassung und Regelung von Software Updates bei in Betrieb befindlichen Fahrzeugen sind nicht harmonisiert. Dies erschwert einen einheitlichen, grenzüberschreitenden Datenaustausch. Zudem müssen zwei bislang weitgehend getrennte Rechtskreise – das Inverkehrbringen neuer Fahrzeuge (Fahrzeugtypgenehmigung) und das Zulassungsrecht für bereits registrierte Fahrzeuge – stärker aufeinander abgestimmt werden.

Handlungsempfehlungen zur zügigen Umsetzung der digitalen Fahrzeugakte

Um die digitale Fahrzeugakte zeitnah zu realisieren, sind aus Sicht des TÜV-Verbands folgende Maßnahmen wesentlich:

1. **Rechtsgrundlagen modernisieren und harmonisieren:**
   Die verpflichtende Einführung digitaler CoC ab 2026 schafft eine wichtige Grundlage. Allerdings müssen die Verknüpfungen zwischen Zulassungsrecht und Software-Update-Management (UN-Regelung Nr. 156) klar geregelt werden, um eine einheitliche digitale Verwaltung zu gewährleisten.
2. **Zentrales Fahrzeugregister auf EU-Ebene etablieren:**
   Ein einheitliches Register für Fahrzeugdaten würde nationale Insellösungen vermeiden und den Austausch zwischen Behörden, Prüfstellen und Herstellern in den Mitgliedsstaaten erheblich erleichtern. Dies ist essenziell, um Datenbrüche zu verhindern und Manipulationen zu erschweren.
3. **Technische und datenschutzrechtliche Absicherung gewährleisten:**
   Die sichere Übertragung und Speicherung sensibler Fahrzeugdaten muss unter Einhaltung der DSGVO-Standards erfolgen. Gleichzeitig sind digitale Signaturen und Integritätschecks erforderlich, um Manipulationen an Fahrzeugdaten zu verhindern.
4. **Harmonisierung der Update- und Genehmigungsprozesse in der EU:**
   Während Deutschland bereits ein Kategorienmodell für softwarebasierte Änderungen nach der Zulassung entwickelt hat, fehlen in anderen EU-Staaten vergleichbare Strukturen. Eine abgestimmte Regulierung in der EU würde Verwaltungsaufwand reduzieren und die Sicherheit erhöhen.
5. **Bestehende Digitalisierungsprojekte als Vorbild nutzen:**
   Die bereits begonnenen Initiativen, wie die elektronische Fahrzeugzulassung oder die Digitalisierung von Fahrzeugpapieren, sollten konsequent weiterentwickelt und auf die dFZA ausgeweitet werden.

Die digitale Fahrzeugakte bietet enorme Chancen für Transparenz, Effizienz und Sicherheit im Fahrzeuglebenszyklus. Um diese Potenziale zu heben, braucht es eine enge Zusammenarbeit zwischen Politik, Industrie und Überwachungsinstitutionen. Eine zügige Umsetzung der notwendigen regulatorischen Anpassungen sowie die Schaffung eines zentralen digitalen Registers sind entscheidend, um die dFZA als europäisches Best-Practice-Modell zu etablieren.

Zugang zu fahrzeuggenerierten Daten: Klare Regulierung statt fehlendes Vertrauen in die Datennutzung – Sicherheit, Innovation und Gleichberechtigung gewährleisten

Die zunehmende Digitalisierung und Vernetzung von Fahrzeugen führt zu einer exponentiellen Zunahme von Daten, die im Fahrzeug selbst generiert und verarbeitet werden. Sowohl im automatisierten als auch im konventionellen Fahrbetrieb fallen zahlreiche Informationen an – von Fahrzustands- und Positionsdaten über Sensordaten (z.B. Radar, Lidar) bis hin zu Daten über den Fahrzeugzustand (z.B. Batteriestatus, Bremssysteme) und Softwareversionen elektronischer Steuergeräte. Diese fahrzeuggenerierten Daten sind von hoher Relevanz für die periodisch technische Überwachung der Kraftfahrzeuge, für die Abnahme von Fahrzeugänderungen, allgemeinen Sicherheitsdiagnosen und der Weiterentwicklung KI-basierter Systeme bzw. insgesamt für die Nachverfolgbarkeit von sicherheits- und umweltrelevanten Veränderungen im Lebenszyklus eines Kraftfahrzeugs. Dennoch sind der Zugang und die Nutzung dieser Daten bislang nicht hinreichend klar geregelt, was sowohl Innovationshemmnisse als auch Sicherheitsrisiken nach sich zieht.

Für eine effiziente Regulierung ist zunächst eine differenzierte Betrachtung der verschiedenen Datenkategorien notwendig:

- Diagnosedaten: Technische Daten zum Zustand und zur Funktionsfähigkeit des Fahrzeugs
- Nutzerdaten: Informationen zu Fahrverhalten oder persönliche Einstellungen
- Originäre Fahrzeugdaten: kontinuierlich durch Sensorik und Steuergeräte erfasste Rohdaten
- Aggregierte Daten: Zusammengefasste und anonymisierte Datensätze (z.B. für Forschung und Entwicklung nutzbar)

Nur ein datenschutzkonformer, direkter und standardisierter Zugang zu diesen Daten – exklusive der Nutzerdaten – ermöglicht hoheitliche Fahrzeugüberprüfungen durch unabhängige Stellen und fördert die Entwicklung innovativer Mobilitätslösungen. Die EU-Kommission erkennt in ihrem „Industrial Action Plan for the European automotive sector" (COM(2025) 95) zwar die Notwendigkeit eines gesetzlichen Rahmens für den „Access to Vehicle Data" an und plant legislative Initiativen, falls notwendig. Vorgesehen sind jedoch lediglich rechtlich unverbindliche Leitlinien („Guidance") als Begleitdokument

zum Inkrafttreten des Data Acts am 12. September 2025, der nur allgemeine Zugangsrechte für datenproduzierende Geräte und Produkte definiert. Dieser Ansatz ist unzureichend, da zentrale Aspekte des Zugangs zu fahrzeuggenerierten Daten ungelöst bleiben:

- **Fehlende Standardisierung der Schnittstellen:** Fahrzeuge sind hochkomplexe, softwaregesteuerte Systeme mit kontinuierlichen Update-Prozessen. Ohne einheitliche, interoperable Standards für On-Board- und Off-Board-Zugriffe sowie Sicherheitsmechanismen bleibt der Datenzugang ineffizient und uneinheitlich.
- **Unzureichende Einbindung unabhängiger Prüfstellen:** Während die EU-Kommission „mehr Geschäftsmöglichkeiten für alle Akteure" verspricht, fehlen klare Regelungen, wie hoheitlich tätige Prüf- und Überwachungsorganisationen gleichberechtigten und zeitnahen Zugang zu sicherheitsrelevanten Daten erhalten sollen.
- **Mangelnde Berücksichtigung der spezifischen Anforderungen der Automobilbranche:** Die Anforderungen an den Zugang zu Fahrzeugdaten sind komplexer als in anderen IoT-Bereichen (z.B. Smart Home). Besonders KI-gestützte Fahrfunktionen und sicherheitskritische Steuergeräte erfordern eine kontinuierliche Überwachung (SOTIF-, ASIL- und Cybersecurity-Compliance).
- **Keine verbindliche Regelung für laufende Compliance-Prüfungen:** Ohne Regulierung bleibt unklar, wie bereits jetzt bestehende Sicherheits- und Transparenzanforderungen – insbesondere für Software Updates – eingehalten werden sollen. Die technologische Entwicklung schreitet schneller voran, als der regulatorische Prozess darauf reagiert.

Um den Herausforderungen im Bereich des sicheren und standardisierten Fahrzeug-Datenzugangs zu begegnen und einen rechtssicheren Rahmen zu schaffen, sind gezielte Maßnahmen erforderlich:

1. Ein zentraler Punkt ist die Einführung standardisierter, sicherer und interoperabler Schnittstellen. Einheitliche technische Anforderungen für den Datenzugang müssen verbindlich festgelegt werden, um eine herstellerübergreifende Nutzung zu ermöglichen. Nur so lassen sich unabhängige Prüfungen und datenbasierte Mobilitätsservices effektiv umsetzen.
2. Ebenso essenziell ist ein herstellerunabhängiger und gleichberechtigter Zugang zu relevanten Daten für die Fahrzeugüberwachung. Akteure wie Prüfstellen, Flottenmanager oder Reparaturbetriebe dürfen nicht vom Wohlwollen der Fahrzeughersteller abhängig sein. Deshalb müssen verbindliche On-Board-Zugänge gewährleistet werden, die sicherheitskritische Informationen in Echtzeit diskriminierungsfrei verfügbar machen.
3. Schließlich bedarf es einer engen Koordinierung mit bestehenden Rechtsvorgaben. Die unterschiedlichen gesetzlichen Regelungen – darunter die DSGVO, der Data Act, das Typgenehmigungsrecht, der EU Cyber Resilience Act sowie die UNECE-Regelungen – müssen harmonisiert werden, um Rechtsunsicherheiten und mögliche Widersprüche zu vermeiden.

Die aktuellen Pläne der EU-Kommission für den Zugang zu fahrzeuggenerierten Daten greifen zu kurz. Eine bloße Erweiterung des Data Acts reicht nicht aus um die spezifischen Herausforderungen der Automobilbranche zu adressieren. Es ist dringend erforderlich, dass Politik, Gesetzgeber und Industrie rasch einen durchsetzbaren Rechtsrahmen schaffen. Dieser muss über rechtliche unverbindliche Leitlinien deutlich hinausgehen und standardisierte Schnittstellen, gleichberechtigten Datenzugang sowie Sicherheitsvorgaben klar regeln. Ein transparent geregelter Datenzugang stärkt das Vertrauen in vernetzte Fahrzeuge, fördert Innovationen und sichert die Wettbewerbsfähigkeit der europäischen Automobilindustrie.

Integrativer Datenschutz bei der Zulassung autonomer Mobilitätskonzepte

Obwohl der Rechtsrahmen für Kraftfahrzeuge mit „autonomen" Fahrfunktionen in Deutschland und Europa bereits geschaffen wurde, sind spezifische datenschutzrechtliche Regelungen für die Verarbeitung personenbezogener Daten, aus in autonomen Systemen generierten Mobilitäts- und Fahrzeugdaten, bislang unzureichend berücksichtigt. Datenschutz und Datennutzung dürfen sich nicht gegenseitig behindern.

Herausforderungen im Datenschutz

Moderne Fahrzeuge erfassen eine Vielzahl an Daten – von Fahrzeug- und Bediendaten über Umgebungs- und Infrastrukturdaten bis hin zu Ereignis- sowie Infotainment-Daten. Diese Daten sind nicht nur notwendig für die Gewährleistung der Betriebssicherheit und die kontinuierliche Aufrechterhaltung der Assistenzsysteme und automatisierten Fahrsysteme, sondern bieten auch Potenziale zur Verbesserung der Verkehrssicherheit, Optimierung von Wartungsdiensten oder zur Entwicklung neuer Serviceangebote. Allerdings kollidiert das prinzipielle Data-Sharing mit den Vorgaben der DSGVO, die, basierend auf dem Grundsatz der Datenminimierung, die Souveränität des Betroffenen schützen soll. Insbesondere Fahrzeugidentifikationsnummern (FIN) und deren Verknüpfung mit technischen Daten bergen das Risiko, Rückschlüsse auf Fahrzeughalter:innen zuzulassen und damit personenbezogene Daten im Sinne der DSGVO zu erzeugen.

Handlungsempfehlungen für eine datenschutzkonforme Genehmigung

Um einerseits den technischen Fortschritt und die Verkehrssicherheit zu fördern und andererseits den Anforderungen des Datenschutzrechts gerecht zu werden, sollten folgende Maßnahmen in einer sektorspezifischen Regelung zum Datenrecht im Automobilsektor einfließen:

- **Technische und organisatorische Maßnahmen**

In der Automobilbranche bestimmt weitgehend das Fahrzeugdesign, welche Daten generiert, verarbeitet und gesammelt werden. Dies gilt umso mehr, je höher der Grad an Konnektivität, Kapazität und Automatisierung ist. Fahrzeuge mit autonomen Fahrfunktionen müssen so konstruiert sein, dass durch technische und organisatorische Maßnahmen die datenschutzrechtlichen Anforderungen an die Verarbeitung und Übermittlung der durch Nutzung des Fahrzeugs generierten Daten eingehalten werden. Die Einhaltung dieser Anforderungen müssen im Lebenszyklus des Kfz regelmäßig überprüft werden.

- **Datensparsamkeit und Anonymisierung**
  Vor einer Weitergabe von Daten sollte, soweit technisch möglich, auf Anonymisierungs- oder Pseudonymisierungstechniken zurückgegriffen werden. Es empfiehlt sich, gesetzliche Kriterien oder eine Vermutung für einen ausreichenden Grad der Anonymisierung zu definieren. Zusätzlich sind kryptographische Verfahren anzuwenden, um die Integrität und Vertraulichkeit der Daten zu sichern.

- **Einwilligungsmanagement und Datentreuhänderschaft**
  Zur Effektivierung des Datenschutzes sollten unabhängige Datenvermittlungsdienste eingerichtet werden, die als zentrale Instanz das Einwilligungsmanagement übernehmen. Diese Dienste ermöglichen es dem Fahrzeughalter oder Nutzer, ihre Präferenzen für zukünftige Datenzugriffe festzulegen. Darüber hinaus können sie als Datentreuhänder fungieren, um den kontrollierten Zugang Dritter zu gewährleisten – etwa für Zwecke wie Unfallforschung oder Verkehrssicherheitsanalysen.

- **Verzahnung von Datenschutz und öffentlichem Interesse**
  Neben der Sicherstellung der individuellen Datensouveränität ist es erforderlich, verbindliche Regelungen für den Datenzugang im öffentlichen Interesse (z.B. für Umweltschutz oder Verkehrssicherheit) zu schaffen. Hier besteht dringender Handlungsbedarf, um die bisher weitgehend auf freiwilliger Basis regelbaren Datenzugangsrechte auch für Behörden verbindlich zu machen.

Eine datenschutzkonforme Genehmigung von Fahrzeugen mit autonomen Fahrfunktionen erfordert eine enge Abstimmung zwischen technischen Standards und rechtlichen Vorgaben. Die Hersteller tragen dabei eine Schlüsselrolle – von der fahrzeugseitigen Datenerfassung bis hin zur Bereitstellung sicherer Schnittstellen. Gleichzeitig müssen gesetzliche Regelungen dafür sorgen, dass der Schutz personenbezogener Daten gewährleistet ist, ohne den technischen Fortschritt und die innovativen Nutzungsmöglichkeiten moderner Mobilität zu hemmen. Eine klare gesetzliche Verankerung der datenschutzspezifischen Maßnahmen und des Einwilligungsmanagements ist dabei unerlässlich, um langfristig ein ausgewogenes Verhältnis zwischen individuellem Datenschutz und öffentlichem Interesse zu erreichen.

Anpassung der Periodischen Fahrzeugüberwachung an Elektromobilität und moderne, hochentwickelte Fahrzeugassistenzsysteme

Die regelmäßige technische Überwachung von Kraftahrzeugen (HU/PTI) ist ein essenzielles Instrument zur Gewährleistung der Verkehrssicherheit und zur Reduzierung umweltbelastender Emissionen. Mit der Veröffentlichung eines Vorschlags für die Überarbeitung der EU-Richtlinie zur periodisch technischen Fahrzeugüberwachung (COM(2025) 180 final) hat die EU-Kommission erkannt, dass die bestehenden HU-Vorgaben an die technologischen Entwicklungen im Fahrzeugbau angepasst werden müssen. Insbesondere die periodische Überwachung von Elektrofahrzeugen, die moderne Abgasprüfungen und die Überprüfung elektronischer Fahrzeugsysteme erfordern präzisere Prüfmethoden und eine bessere Datenverfügbarkeit. Zugleich ist eine engere Abstimmung (regulatorische Kohärenz) mit der Typgenehmigung essenziell, um die Verkehrssicherheit nachhaltig zu gewährleisten.

Anpassung der PTI an die Elektromobilität

Für Elektro- und Hybridfahrzeuge sind spezifische Prüfpunkte erforderlich, die über die bestehenden Überprüfungen hinausgehen. Dazu zählen insbesondere:

- **Sicherheits- und Umweltaspekte von Hochvoltsystemen:** Die Überprüfung der Batteriesicherheit, z.B. durch Isolations- und Potentialausgleichsmessungen, aber auch die Prüfung der Software des Batterie-Management-Systeme (BMS) müssen systematisch erfolgen. Eine rein visuelle Prüfung reicht bei diesen sicherheitskritischen Hochvoltsystemen nicht aus.
- **Spezielle Prüfverfahren:** Die Messung des Isolationswiderstands und des Potentialausgleichs kann dazu beitragen, Gefahren wie Stromschläge oder Brände frühzeitig zu erkennen. Zudem wäre eine Prüfverfahren bei Be- und Entladen während der PTI erforderlich, um potenzielle Störungen in den Batteriezellen oder Fehlfunktionen von Ladegeräten und Batteriesteuerungen aufzudecken.
- **Batteriezustand & Sicherheitsbewertung:** Langfristig sollte untersucht werden, wie der allgemeine Sicherheitszustand von Hochvoltbatterien bewertet werden kann. Wichtige Parameter wie Softwareversionen des BMS, mögliche Manipulationen oder Hochvoltsicherheitsaspekte müssen in die Prüfung einbezogen werden. Bereits auf Ebene der Typgenehmigung sollte die Prüfbarkeit sicherheitsrelevanter Batteriedaten gewährleistet werden.
- **Datenzugang:** Um eine aussagekräftige PTI durchzuführen, ist ein standardisierter, diskriminierungsfreier Zugang zu Fahrzeugdaten und vor allem Batterie-Zelldaten notwendig. Dieser muss herstellerunabhängig geregelt sein, um Manipulationen vorzubeugen und die Effizienz der Prüfungen zu erhöhen.

Verstärkte Prüfung von Sicherheitssystemen und Emissionskontrolle

Neben der Elektromobilität müssen auch moderne Sicherheits- und Umweltaspekte stärker in die PTI einfließen:

- **Elektronisch geregelte sicherheitsrelevante Systeme:** Die Prüfung von Fahrerassistenzsystemen (ADAS), Bremsassistenten und automatisierten Fahrfunktionen muss über die reine Sicht- und Verbauprüfung sowie Untersuchung der Funktion und Wirkung über die elektronische Fahrzeugschnittstellehinausgehen. Es muss nachweislich unter Zuhilfenahme zusätzlicher geeigneter Prüfmittel geprüft werden, ob diese Systeme und ihre Selbstüberwachung ordnungsgemäß hinsichtlich ihrer Funktion und Wirkung arbeiten können. Somit stehen die Umfeldsensorprüfungen im Fokus. Beispiele aus der HU und der Marktüberwachung zeigen, dass z.B. degradierte Sensoren die Funktionen von Fahrerassistenzsystemen beeinflussen können, ohne dass die Eigendiagnose dies erkennt.
- **Erweiterte Abgasmessungen:** Für Fahrzeuge mit Verbrennungsmotor – auch Hybridfahrzeuge – sollten präzisere Prüfmethoden wie die Partikelanzahlmessung oder NOx-Tests eingeführt werden. Zudem ist eine engere Abstimmung mit den Emissionsvorgaben der Typgenehmigung (z.B. Euro-7-Standard) erforderlich, um realitätsnahe Werte sicherzustellen.

Zugang zu Software und On-Board-Diagnose (OBD)

Da immer mehr Fahrzeugfunktionen softwaregesteuert sind, ist ein sicherer, standardisierter Zugang zu den Steuergeräten und zu Echtzeitdaten an der elektronischen Fahrzeugschnittstelle erforderlich. Es gilt insbesondere Prüfmodi für Assistenzsysteme zu ermöglichen. Langfristig müssen Manipulationen – beispielsweise durch nicht genehmigte Software-Updates oder das Deaktivieren von Warnfunktionen – über die PTI nachweisbar sein.

Zusammenspiel mit der Typgenehmigung

Viele HU/PTI-relevante Aspekte sollten bereits bei der Typgenehmigung berücksichtigt werden. Dazu zählen die klare Definition von Prüfmethoden, der Zugang zu sicherheitskritischen Fahrzeugdaten sowie die Bereitstellung eindeutiger Messpunkte für Hochvoltprüfungen. Dadurch wird sichergestellt, dass Prüforganisationen eine zuverlässige und effiziente Überprüfung im Rahmen der HU durchführen können, ohne Fahrzeuge aufwendig zu zerlegen.

Virtuelle Prüfmethoden in der Typprüfung: Effizienz steigern, Sicherheit gewährleisten

Aufgrund der hohen Komplexität moderner Fahrzeuge und Fahrzeugsysteme ist es nicht mehr möglich, ihre Konformität mit den existierenden Typprüfvorschriften auf herkömmliche Weise allein durch praktische Prüfungen nachzuweisen. Eine zentrale Rolle in der Absicherungsstrategie für Assistenzsysteme und automatisierte Fahrfunktionen nehmen Computersimulationen ein. Insbesondere für Szenarien, die auf einer Teststrecke stattfinden, unter realen Fahrbedingungen oder auf dem Prüfstand schwierig sind und nicht unter Ausschluss der Gefährdung von Personen durchgeführt werden können oder die mit hoher Varianz auftreten, bietet sich der Einsatz von Simulationswerkzeugen und mathematischen Modellen an als ergänzende Methoden zur Nachweisführung für die Leistungsfähigkeit der Prüfgegenstände. Die Einführung solcher virtuellen Prüfmethoden bei der Typprüfung von Fahrzeugen und Fahrzeugsystemen bietet somit großes Potenzial zur Steigerung der Effizienz und Innovationsfähigkeit sowie der Beibehaltung hoher Sicherheitsstandards – ohne dabei Menschenleben zu gefährden.

Obwohl virtuelle Tests in der Automobilentwicklung zunehmend an Bedeutung gewinnen, ist der reale Test aber noch lange nicht überflüssig. Zwar bieten Simulationen zahlreiche Vorteile wie eine sichere, schnelle und reproduzierbare Durchführung von Versuchen. Komplexe Systeme, die Interaktionen von Menschen mit Produkten sowie unvorhersehbare Ereignisse lassen sich aber nur eingeschränkt virtuell abbilden. Daher werden auch weiterhin reale Erprobungen, Versuche und Tests notwendig bleiben.

Der TÜV-Verband empfiehlt eine klare Unterscheidung zwischen drei virtuellen ergänzenden Prüfmethoden, die entsprechend der Komplexität und spezifischen Anforderungen der Prüfobjekte gezielt eingesetzt werden sollten. Methode 1 eignet sich für Prüfungen mit geringer Variabilität, Methode 2 für Prüfungen, die bereits klar reguliert sind, und Methode 3 für komplexe Systeme wie automatisierte Fahrfunktionen, die eine umfassende Nachweisführung erfordern.

Zentral für den Einsatz dieser Methoden ist eine glaubwürdige und unabhängige Bewertung der verwendeten Simulationswerkzeuge und -modelle und Ihres vorschriftsmäßigen Einsatzes durch Technische Dienste. Diese müssen die Validierung und Eignung der Simulationen überprüfen. Die Methodik des virtuellen Prüfens gilt es auf der Ebene der UNECE verstärkt zu etablieren, so dass diese in den jeweiligen UN-Regelungen anwendbar ist, ohne jeweils hohe Aufwände zu erzeugen. Beim Anbau von Leuchten, Kennzeichen oder Türen, macht virtuelles Prüfen beispielsweise keinen Sinn.

Der TÜV-Verband unterstreicht dabei insbesondere die Unabhängigkeit, Unparteilichkeit und kontinuierliche Kompetenzprüfung durch Technischen Dienste als essenzielle Kriterien für den erfolgreichen Einsatz virtueller Prüfverfahren. Außerdem müssen Anpassungen zur Integration virtueller Prüfmethoden kurzfristig umgesetzt werden, um eine einheitliche und transparente Regelanwendung in Europa sicherzustellen. Dies betrifft insbesondere die Klarstellung von Anforderungen hinsichtlich Genauigkeit, Korrektheit, Prozesskonformität und Kritikalität der eingesetzten Modelle und Simulationsergebnisse.

Zwischen Regulierung und Praxis: Cybersecurity als Pflicht im Fahrzeuglebenszyklus

Automobilhersteller sehen sich im Bereich der Cybersicherheit mit einer Vielzahl regulatorischer Anforderungen konfrontiert, die Voraussetzung für die Typgenehmigung neuer Kraftfahrzeuge sind. Diese Anforderungen zielen darauf ab, moderne Fahrzeuge gegen die wachsende Zahl digitaler Angriffe abzusichern und sind sowohl in nationalen Vorgaben als auch in internationalen Standards wie der UN-Regelung Nr.155 und der ISO/SAE 21434 verankert.

Kernanforderung für die Typgenehmigung ist die Einrichtung eines Cybersecurity-Managementsystems (CSMS), dass alle Phasen des Fahrzeuglebenszyklus abdeckt – von der Konzeption über die Produktion bis hin zum Betrieb und der späteren Außerbetriebssetzung. Diese Verpflichtung ergibt sich unmittelbar aus der UN-Regelung Nr. 155, die als rechtlich bindende Vorgabe in der EU und damit auch in Deutschland gilt. Der Aufbau eines CSMS ist nicht nur formaler Bestandteil der Zulassung, sondern stellt die strukturelle Grundlage dar, um Risiken systematisch zu identifizieren und geeignete Schutzmaßnahmen umzusetzen.

Hersteller sind verpflichtet, eine systematische Risikoanalyse durchzuführen – üblicherweise in Form einer Gefahren- und Risikoanalyse (Threat Analysis and Risk Assessment - TARA). Diese Analyse bildet die Grundlage für die Ableitung konkreter Testfälle, die sowohl funktionale Sicherheitsaspekte als auch mögliche Angriffsszenarien abdecken. Die Tests müssen dokumentiert und reproduzierbar sein; das Kraftfahrt-Bundesamt (KBA) verlangt dabei mindestens einen praktischen Nachweis pro Regelwerk (R.155/R.156), entweder durch eigene Tests oder durch Begutachtung eines Technischen Dienstes. Zur Nachweisführung gehören neben detaillierten Risikoanalysen auch Testpläne, umfassende Berichte mit erwarteten und tatsächlichen Ergebnissen sowie Begründungen für etwaige Abweichungen. Die Reproduzierbarkeit muss über einen Zeitraum von mindestens zehn Jahren sichergestellt werden, was hohe Anforderungen an Dokumentation und Testumgebungen stellt.

Zusätzlich zu den verbindlichen Anforderungen der UNECE orientieren sich Hersteller an der ISO/SAE 21434. Dieser Standard liefert einen methodischen Rahmen für die Cybersicherheit über den gesamten Lebenszyklus hinweg, ist jedoch im Gegensatz zur UN-Regelung Nr.155 nicht rechtlich bindend, sondern als Best-Practice-Leitlinie zu verstehen. Dennoch wird er in der Praxis breit angewendet, insbesondere bei der Testfallableitung und der Implementierung von Schutzmaßnahmen. Die Einbindung Technischer Dienste ist ein weiterer zentraler Aspekt. Diese unabhängigen Prüfstellen kontrollieren die Wirksamkeit der Sicherheitsmaßnahmen und bestätigen die Einhaltung der regulatorischen Anforderungen. Dabei zeigt sich in der Praxis ein klarer Fokus auf funktionale Sicherheitstests und Penetrationstests, mit einer starken Orientierung an modell- und risikobasierten Ansätzen. Systemübergreifende Tests bleiben hingegen die Ausnahme.

Regulierungsperspektiven und der EU Cyber Resilience Act

Ein zukünftiger Regulierungsaspekt ergibt sich aus dem geplanten EU Cyber Resilience Act (CRA) (EU 2024/2847), der digitale Produkte und Dienstleistungen reguliert, die außerhalb der EU-Verordnung 2019/2144 (GSR-II Fahrzeugtypgenehmigung) liegen. Der CRA sieht deutlich strengere Anforderungen an die kontinuierliche Überprüfung und Aktualisierung digitaler Systeme vor. Damit entsteht eine doppelte Regulierungslandschaft: Der Fahrzeugkern bleibt unter UN-Regelung Nr. 155 und ISO/SAE 21434, digitale Zusatzsysteme unterliegen dem CRA.

Dies führt zu Herausforderungen: Hersteller müssen zwei Regime parallel bedienen, was Überschneidungen und erhöhte administrative Belastungen nach sich zieht. Hier ist eine klare Abgrenzung erforderlich, welche Systeme als „Fahrzeugkern" gemäß der EU-VO 2019/2144 gelten und welche unter den CRA fallen. Nur durch eine harmonisierte Abstimmung lässt sich Rechtssicherheit schaffen.

Wichtig ist, dass die Systembegutachtung und Genehmigung aber auch von den anderen Typgenehmigungsstellen anerkannt wird. Derzeit ist eine gegenseitige Anerkennung der Managementbewertung nicht etabliert. Angesichts dieser Lage sind politische Maßnahmen nötig, zu denen bereits Mario Draghi in seinem Bericht zur europäischen Wettbewerbsfähigkeit anriet:

- **Klare Abgrenzung und Harmonisierung:** Es braucht eine präzise Definition der Anwendungsbereiche von UN-Regelung Nr. 155, ISO/SAE 21434 und CRA. Doppelregelungen müssen vermieden, Schnittstellen klar geregelt werden.
- **EU-weite Governance:** Ein koordinierter europäischer Regulierungsrahmen kann helfen, Inkohärenzen zu vermeiden und den Binnenmarkt zu stärken. Einheitliche Standards reduzieren Aufwand und schaffen Wettbewerbsgleichheit.

Die Anforderungen an Cybersicherheit in der Fahrzeugzulassung sind komplex, aber notwendig. Hersteller müssen robuste Prozesse etablieren, um modernen Bedrohungen zu begegnen. Gleichzeitig besteht politischer Handlungsbedarf, um Doppelregulierungen zu vermeiden und klare, umsetzbare Vorgaben zu schaffen. Nur so kann Cybersecurity wirksam und nachhaltig in die Fahrzeugentwicklung und Lebenszyklus integriert werden.

Autor und Ansprechpartner

Richard Goebelt
Fachbereichsleiter Fahrzeug & Mobilität
E-Mail: richard.goebelt@tuev-verband.de
Tel. +49 30 760095 350
www.tuev-verband.de

Über den TÜV-Verband: Als TÜV-Verband e.V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

Herausgeber
TÜV-Verband e.V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095 400
E-Mail: berlin@tuev-verband.de

www.tuev-verband.de