Bundesministerium
Innovation, Mobilität
und Infrastruktur

bmimi.gv.at

Peter Hanke
Bundesminister

ministerbuero@bmimi.gv.at
+43 1 711 62-658000
Radetzkystraße 2, 1030 Wien
Österreich

An den
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-0.955.359

19. Jänner 2026

Sehr geehrter Herr Präsident!

Die Abgeordneten zum Nationalrat Mag.ª Giuliani-Sterrer, BA und weitere Abgeordnete haben am 19. November 2025 unter der **Nr. 3925/J** eine schriftliche parlamentarische Anfrage betreffend „Gefahr für Datenschutz und nationale Sicherheit durch digitale Fahrzeuge“ an mich gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu den Fragen 1, 8, 9, 12, 19, 20 und 23:

- *Welche Prüfmechanismen und Zulassungskriterien bestehen aktuell, um sicherzustellen, dass Kraftfahrzeuge und digitale Endgeräte ausländischer Hersteller keine datenschutzrechtlichen oder sicherheitsrelevanten Risiken für Bürger und Staat darstellen?*
- *Welche Maßnahmen setzt die Bundesregierung, um zu verhindern, dass personenbezogene Daten aus Österreich durch ausländische Hersteller oder über deren Cloudsysteme ohne Wissen und Zustimmung der Betroffenen ins Ausland transferiert werden?*
- *Welche Vorgaben bestehen für Anbieter von digitalen Diensten und Fahrzeugen, um einen Zugriff Dritter auf Fahrzeugdaten, Standortinformationen, Kommunikations- und Nutzungsdaten zu verhindern?*
- *Welche Vereinbarungen bestehen mit internationalen Herstellern, um österreichischen Behörden im Anlassfall Zugang zu Daten oder technischen Schnittstellen von Fahrzeugen zu ermöglichen?*
- *Wie wird geprüft, ob Funktionen zur Fernsteuerung, Abschaltung oder Überwachung von Fahrzeugen oder Endgeräten, etwa durch GPS-Blockierung oder digitale Zugangssperren, im Krisen- oder Kriegsfall eine Gefahr für Sicherheit und öffentliche Ordnung darstellen können?*
- *Welche Kontrollen bestehen, um zu verhindern, dass über digitale Schnittstellen von Fahrzeugen Manipulationen, Sabotageakte oder unerlaubte Eingriffe vorgenommen werden?*

- *Welche rechtlichen oder technischen Hürden bestehen derzeit, um im Anlassfall die digitale Abschaltung oder Manipulation von Fahrzeugen durch ausländische Akteure nachzuweisen und zu verhindern?*

Die EU-Verordnung 858/2018 enthält Vorschriften für die technische Beschaffenheit von Kraftfahrzeugen, die an die Herstellenden adressiert sind und von diesen einzuhalten sind. Zusätzlich sind die europäischen Datenschutzbestimmungen der Datenschutz-Grundverordnung (DSGVO) und die geltenden Regeln des Datenschutzgesetzes einzuhalten.

IT-Sicherheitsrelevante Risiken werden durch die UN-Regelung Nr. 155 hinsichtlich Cybersicherheit abgedeckt, die von allen Kraftfahrzeugen und Herstellern zu erfüllen sind. Hersteller haben ein Cybersicherheitsmanagementsystem (CSMS) nachzuweisen, die Voraussetzung für die Typengenehmigung ist. Weiters sind für jeden Fahrzeugtypen Maßnahmen zu treffen, um Cyberangriffe zu erkennen und zu verhindern.

Zu den Fragen 2 und 4:

- *Inwieweit werden bei der Beschaffung von Fahrzeugen und digitalen Systemen für öffentliche Stellen gezielte Risikobewertungen hinsichtlich des Zugriffs ausländischer Konzerne, Geheimdienste oder Regierungen auf in Österreich erhobene Daten vorgenommen?*
- *Welche Anforderungen stellt die Bundesregierung an Ausschreibungen und öffentliche Vergaben, um sicherzustellen, dass bei staatlichen Aufträgen nur Fahrzeuge und Systeme mit höchsten Datenschutz- und IT-Sicherheitsstandards beschafft werden?*

Mein Ressort stellt bei Vorhaben im eigenen Wirkungsbereich sicher, dass Beschaffungsvorgänge gemäß den Vorgaben des Bundesvergabegesetzes durchgeführt werden und den Vorgaben der Datenschutz-Grundverordnung (DSGVO), des österreichischen Datenschutzrechts sowie nationalen und europäischen Sicherheitsstandards entsprechen.

Zu Frage 3:

- *Wie viele Kraftfahrzeuge, die mit Telematiksystemen, integrierten SIM-Karten oder internetfähigen Sensoren ausgerüstet sind, wurden seit 2020 von öffentlichen Stellen angeschafft?*
    a. *Aus welchen Herstellungsländern kommen diese?*

Meinem Ressort liegen diesbezüglich keine Informationen vor.

Zu den Fragen 5 und 6:

- *Wie wird die laufende Überprüfung und bereits beschaffter Fahrzeuge und digitaler Systeme hinsichtlich möglicher Sicherheitslücken, Missbrauchsgefahren oder Manipulationsmöglichkeiten organisiert?*
- *Gibt es technische oder rechtliche Mindeststandards, die ausländische Hersteller erfüllen müssen, um auf dem österreichischen Markt zugelassen zu werden?*
    a. *Wenn ja, welche?*
    b. *Wie wird die Einhaltung dieser Mindeststandards kontrolliert?*

Die EU-Typengenehmigungsverordnungen regeln die einzuhaltenden Mindeststandards. Deren Einhaltung ist im Rahmen des Typengenehmigungsverfahrens nachzuweisen und wird durch die Typengenehmigungsbehörden überprüft. Darüber hinaus erfolgen im Rahmen der Marktüberwachung Kontrollen durch die Marktüberwachungsbehörden der Mitgliedstaaten.

Zu Frage 7:

- *Welche Rolle spielen österreichische oder europäische Zulassungsstellen bei der Überprüfung der digitalen Komponenten, bevor ein Fahrzeugmodell für den Straßenverkehr zugelassen wird?*

Die Genehmigungsbehörden müssen die Einhaltung der bereits genannten Typengenehmigungsvorschriften überprüfen. Dies umfasst auch die in Kraftfahrzeugen verbauten digitalen Komponenten, soweit für diese kraftfahrrechtliche Vorschriften bestehen.

Zu den Fragen 10, 11, 13 und 14 sowie 16 und 18:

- *Inwieweit wird kontrolliert, ob Daten von österreichischen Nutzern, die durch ausländische Fahrzeughersteller oder App-Anbieter erhoben werden, tatsächlich ausschließlich innerhalb der EU gespeichert und verarbeitet werden?*
- *Welche konkreten Erkenntnisse hat die Bundesregierung über den Datenabfluss nach China, in die USA oder andere Drittstaaten im Zusammenhang mit der Nutzung moderner Kraftfahrzeuge und Fahrzeug-Apps?*
- *Wie stellt die Bundesregierung sicher, dass Bürger umfassend und transparent über die Datenerhebung, Datenverwendung und ihre Rechte durch Fahrzeughersteller und App-Anbieter informiert werden?*
- *Wie viele Beschwerden oder Hinweise zu Datenschutzverletzungen im Zusammenhang mit digital vernetzten Fahrzeugen und Mobilitätsdienstleistungen sind seit 2020 bei österreichischen Behörden eingegangen?*
- *Welche Konsequenzen zieht die Bundesregierung, wenn ein Hersteller nachweislich gegen Datenschutzbestimmungen oder Sicherheitsauflagen verstößt?*
- *Gibt es Pläne, die Rolle und Ressourcen der Datenschutzbehörde im Bereich der Kontrolle ausländischer Digitalprodukte und Fahrzeuge auszubauen?*

Die Einhaltung datenschutzrechtlicher Bestimmungen ist seitens der jeweiligen Unternehmer:innen bzw. App-Anbieter:innen gemäß der gesetzlichen Vorgaben als datenschutzrechtliche Verantwortliche sicherzustellen. Diese treffen auch etwaige Informationsverpflichtungen an die Betroffenen. Angelegenheiten der Datenschutzbehörde, wie beispielsweise die Ahndung von Verstößen oder Einsatz ihrer Ressourcen, fallen nicht in die Kompetenz meines Ressorts.

Zu Frage 15:

- *Gibt es Überlegungen, die gesetzlichen Regelungen für digitale Produkte und Fahrzeuge zu verschärfen, um die nationale Souveränität im Bereich Datenschutz, IT-Sicherheit und kritische Infrastruktur zu stärken?*

Derzeit werden auf EU- und nationaler Ebene die rechtlichen Anforderungen für digitale Produkte und vernetzte Fahrzeuge deutlich verschärft. Wesentliche Neuerungen sind die NIS-2-Richtlinie mit ihrer nationalen Umsetzung im NISG 2026, die erweiterte Pflichten zur Cybersicherheit, Lieferkettensicherheit und Vorfallsmeldung vorsieht, sowie der Cyber Resilience Act, der verbindliche Cybersicherheitsanforderungen für digitale Produkte und

Fahrzeugsoftware festlegt. Ergänzend regelt der EU Data Act (VO (EU) 2023/2854) den kontrollierten und sicheren Zugang zu Fahrzeugdaten. Insgesamt dienen diese Maßnahmen der Stärkung der digitalen Souveränität und des Schutzes kritischer Infrastrukturen.

Zu Frage 17:

- *Gibt es bereits Fälle, in denen Zulassungen entzogen oder Einschränkungen ausgesprochen wurden?*

Meinem Ressort sind keine Fälle von Entziehungen oder Einschränkungen von Typengenehmigungen bekannt.

Zu Frage 21:

- *Wie werden Betreiber von Fahrzeugflotten und Mobilitätsdienstleistern verpflichtet, ihre Kunden vor Missbrauch, Datenklau und Eingriffen durch Dritte zu schützen?*

Betreiber:innen von Fahrzeugflotten und Mobilitätsdienstleister sind aufgrund EU- und nationalrechtlicher Vorgaben verpflichtet, geeignete Maßnahmen zum Schutz vor Missbrauch, Datenabflüssen und unbefugten Eingriffen Dritter zu treffen. Diese Verpflichtungen ergeben sich insbesondere aus der Datenschutz-Grundverordnung (DSGVO) sowie gegebenenfalls aus der NIS-2-Richtlinie und deren nationaler Umsetzung im NISG 2026, welche verbindliche Anforderungen an Cybersicherheit und Risikomanagement vorsehen.

Zu den Fragen 22, 27, 28 und 30:

- *Wie bewertet die Regierung die Gefahr, dass durch die Verbreitung digital gesteuerter Fahrzeuge auch kritische Infrastruktur wie Rettungsdienste, Einsatzfahrzeuge und Energieversorgung im Ernstfall lahmgelegt oder manipuliert werden kann?*
- *Wie bewertet die Bundesregierung das Risiko, dass digitale Überwachung und Datenmissbrauch gezielt zur Erpressung, Diskreditierung oder zur Manipulation politischer Entscheidungsträger eingesetzt werden können?*
- *Welche Kooperationsprojekte bestehen mit anderen EU-Mitgliedstaaten, um den Schutz der europäischen Bürger vor digitalen Risiken durch ausländische Fahrzeug- und Gerätehersteller zu verbessern?*
- *Plant die Bundesregierung, internationale Erkenntnisse und Untersuchungen, wie jene aus Dänemark und Norwegen, künftig systematisch in nationale Risikoanalysen und Schutzmaßnahmen einfließen zu lassen?*
    a. *Wenn nein, warum nicht?*

Die skizzierten Risiken werden von meinem Ressort sehr ernst genommen. Vor dem Hintergrund beobachtbarer Marktveränderungen, insbesondere des zunehmenden Markteintritts von Fahrzeugen aus Drittstaaten sowie aktueller technologischer Entwicklungen, habe ich im Rahmen des TTE-Rates im Dezember 2025 meinen Standpunkt eingebracht, der die Bedenken der Bundesregierung zum Ausdruck bringt. Dabei habe ich die Europäische Kommission aufgefordert, eine Europäische Eisenbahnstrategie vorzulegen, die sich auch mit sicherheitsrelevanten Aspekten in diesem Zusammenhang beschäftigen möge. Gerade im Bereich kritischer Infrastrukturen und bei Fahrzeugen ist es dabei wesentlich, die technologische, wirtschaftliche und regulatorische Souveränität der Nationalstaaten und Europas auch künftig zu wahren.

Zu den Fragen 24 bis 26:

- *Welche Rolle spielen ausländische Geheimdienste oder Terrornetzwerke nach Erkenntnis der Bundesregierung bei der gezielten Ausnutzung digitaler Schwachstellen in vernetzten Fahrzeugen, Mobilitätsdiensten und Kommunikationssystemen?*
- *Gibt es Anhaltspunkte, dass ausländische Geheimdienste, terroristische Gruppen oder andere fremde Akteure in Österreich bereits versucht haben, über digitale Angriffe auf Fahrzeuge, Apps oder Flottenmanagementsysteme Informationen abzugreifen oder Sabotageakte zu begehen?*
- *Wurden im Rahmen der nationalen Sicherheitsstrategie oder in der DSN konkrete Maßnahmen festgelegt, um die Risiken hybrider Kriegsführung im Bereich digitaler Mobilität und Infrastruktur abzuwehren?*
    a. *Wenn ja, welche?*

Diese Fragen fallen nicht in den Zuständigkeitsbereich des Bundesministeriums für Innovation, Mobilität und Infrastruktur.

Zu Frage 29:

- *Welche Rolle spielen europäische Institutionen, etwa die Europäische Agentur für Cybersicherheit (ENISA), bei der Entwicklung und Überwachung von Sicherheitsstandards für digital vernetzte Fahrzeuge?*

Europäische Institutionen übernehmen bei der Entwicklung von Sicherheitsstandards für digital vernetzte Fahrzeuge vor allem eine unterstützende und koordinierende Rolle. Die Europäische Agentur für Cybersicherheit (ENISA) wirkt hierbei insbesondere durch die Erarbeitung von Analysen, Leitlinien und Empfehlungen zur Cybersicherheit vernetzter Systeme mit.

Mit freundlichen Grüßen

Peter Hanke

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNOVATION, MOBILITÄT UND INFRASTRUKTUR
@ AMTSSIGNATUR

Hinweis	Dieses Dokument wurde amtssigniert.
Datum	2026-01-19T16:03:06+01:00
Seriennummer	2069212815
Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at/

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-01-19T16:07:41+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	