3435/AB
vom 19.01.2026 zu 3934/J (XXVIII. GP)

Bundesministerium
Inneres

Mag. Gerhard Karner
Bundesminister

Herrn
Präsidenten des Nationalrates
Dr. Walter Rosenkranz
Parlament
1017 Wien

Geschäftszahl: 2025-1.031.005

Wien, am 19. Jänner 2026

Sehr geehrter Herr Präsident!

Die Abgeordnete zum Nationalrat Mag. Marie-Christine Giuliani-Sterrer, BA hat am 19. November 2025 unter der Nr. **3934/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Gefahr für Datenschutz und nationale Sicherheit durch digitale Fahrzeuge“ gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1 bis 14, 16 bis 18 und 21:

- *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?*
- *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?*
- *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?

- *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?*
- *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?*
- *Welche Rolle spielen österreichische oder europäische Zulassungsstellen bei der Überprüfung der digitalen Komponenten, bevor ein Fahrzeugmodell für den Straßenverkehr zugelassen wird?*
- *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?*
- *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?*
- *Welche Vereinbarungen bestehen mit internationalen Herstellern, um österreichischen Behörden im Anlassfall Zugang zu Daten oder technischen Schnittstellen von Fahrzeugen zu ermöglichen?*
- *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 bereits Fälle, in denen Zulassungen entzogen oder Einschränkungen ausgesprochen wurden?*
- *Gibt es Pläne, die Rolle und Ressourcen der Datenschutzbehörde im Bereich der Kontrolle ausländischer Digitalprodukte und Fahrzeuge auszubauen?*
- *Wie werden Betreiber von Fahrzeugflotten und Mobilitätsdienstleistern verpflichtet, ihre Kunden vor Missbrauch, Datenklau und Eingriffen durch Dritte zu schützen?*

Diese Fragen betreffen keinen Gegenstand der Vollziehung des Bundesministeriums für Inneres und sind daher im Sinne des Artikel 52 Bundes-Verfassungsgesetz in Verbindung mit § 90 Geschäftsordnungsgesetz 1975 keiner Beantwortung durch mich zugänglich.

Zu den Fragen 15 und 27:

- *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?*
- *Wie bewertet die Bundesregierung das Risiko, dass digitale Überwachung und Datenmissbrauch gezielt zur Erpressung, Diskreditierung oder zur Manipulation politischer Entscheidungsträger eingesetzt werden können?*

Meinungen und Einschätzungen unterliegen nicht dem parlamentarischen Interpellationsrecht.

Zu den Fragen 19, 20, 23 bis 26, 28 bis 30:

- *Welche Kontrollen bestehen, um zu verhindern, dass über digitale Schnittstellen von Fahrzeugen Manipulationen, Sabotageakte oder unerlaubte Eingriffe vorgenommen werden?*
- *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 rechtlichen oder technischen Hürden bestehen derzeit, um im Anlassfall die digitale Abschaltung oder Manipulation von Fahrzeugen durch ausländische Akteure nachzuweisen und zu verhindern?*
- *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?*
- *Welche Kooperationsprojekte bestehen mit anderen EU-Mitgliedstaaten, um den Schutz der europäischen Bürger vor digitalen Risiken durch ausländische Fahrzeug- und Gerätehersteller zu verbessern?*
- *Welche Rolle spielen europäische Institutionen, etwa die Europäische Agentur für Cybersicherheit (ENISA), bei der Entwicklung und Überwachung von Sicherheitsstandards für digital vernetzte Fahrzeuge?*
- *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?*

Auf Grund des überwiegenden Geheimhaltungsinteresses der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit, muss von einer Beantwortung der Fragen Abstand genommen werden. Hierzu darf angeführt werden, dass aus jedweder Beantwortung - und sei es auch eine verneinende - Rückschlüsse gezogen werden können. Durch das Bekanntwerden, ob und wenn ja, welche Informationen vorliegen könnten aktuelle oder zukünftige Ermittlungen konterkariert und die Aufgabenerfüllung der Sicherheitsbehörden erschwert bzw. in gewissen Bereichen unmöglich gemacht werden.

Zur Frage 22:

- *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?*

Meinungen und Einschätzungen unterliegen nicht dem parlamentarischen Interpellationsrecht. Aus diesem Grund wird von einer Beantwortung der Frage Abstand genommen.

Gerhard Karner

	Datum/Zeit	2026-01-19T14:41:44+01:00
	Aussteller-Zertifikat	CN=a-sign-corporate-07,OU=a-sign-corporate-07,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	2052038352
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at. Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-01-19T14:44:35+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	