3444/AB
vom 19.01.2026 zu 3931/J (XXVIII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Christian Stocker
Bundeskanzler

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2025-0.953.969

Wien, am 19. Jänner 2026

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Mag. Giuliani-Sterrer, BA, Kolleginnen und Kollegen haben am 19. November 2025 unter der Nr. **3931/J** eine schriftliche parlamentarische Anfrage betreffend „Gefahr für Datenschutz und nationale Sicherheit durch digitale Fahrzeuge“ an mich gerichtet.

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

Zu den Fragen 1 bis 8, 10 bis 12, 14 und 16 bis 30:

1. *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?*
2. *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?*

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?*
4. *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?*
5. *Wie wird die laufende Überprüfung und bereits beschaffter Fahrzeuge und digitaler Systeme hinsichtlich möglicher Sicherheitslücken, Missbrauchsgefahren oder Manipulationsmöglichkeiten organisiert?*
6. *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?*
7. *Welche Rolle spielen österreichische oder europäische Zulassungsstellen bei der Überprüfung der digitalen Komponenten, bevor ein Fahrzeugmodell für den Straßenverkehr zugelassen wird?*
8. *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?*
10. *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?*
11. *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?*
12. *Welche Vereinbarungen bestehen mit internationalen Herstellern, um österreichischen Behörden im Anlassfall Zugang zu Daten oder technischen Schnittstellen von Fahrzeugen zu ermöglichen?*
14. *Wie viele Beschwerden oder Hinweise zu Datenschutzverletzungen im Zusammenhang mit digital vernetzten Fahrzeugen und Mobilitätsdienstleistungen sind seit 2020 bei österreichischen Behörden eingegangen?*
16. *Welche Konsequenzen zieht die Bundesregierung, wenn ein Hersteller nachweislich gegen Datenschutzbestimmungen oder Sicherheitsauflagen verstößt?*
17. *Gibt es bereits Fälle, in denen Zulassungen entzogen oder Einschränkungen ausgesprochen wurden?*

18. *Gibt es Pläne, die Rolle und Ressourcen der Datenschutzbehörde im Bereich der Kontrolle ausländischer Digitalprodukte und Fahrzeuge auszubauen?*
19. *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?*
20. *Welche Kontrollen bestehen, um zu verhindern, dass über digitale Schnittstellen von Fahrzeugen Manipulationen, Sabotageakte oder unerlaubte Eingriffe vorgenommen werden?*
21. *Wie werden Betreiber von Fahrzeugflotten und Mobilitätsdienstleistern verpflichtet, ihre Kunden vor Missbrauch, Datenklau und Eingriffen durch Dritte zu schützen?*
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?*
23. *Welche rechtlichen oder technischen Hürden bestehen derzeit, um im Anlassfall die digitale Abschaltung oder Manipulation von Fahrzeugen durch ausländische Akteure nachzuweisen und zu verhindern?*
24. *Welche Rolle spielen ausländische Geheimdienste oder Terrornetzwerke nach Erkenntnis der Bundesregierung bei der gezielten Ausnutzung digitaler Schwachstellen in vernetzten Fahrzeugen, Mobilitätsdiensten und Kommunikationssystemen?*
25. *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?*
26. *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?*
27. *Wie bewertet die Bundesregierung das Risiko, dass digitale Überwachung und Datenmissbrauch gezielt zur Erpressung, Diskreditierung oder zur Manipulation politischer Entscheidungsträger eingesetzt werden können?*
28. *Welche Kooperationsprojekte bestehen mit anderen EU-Mitgliedstaaten, um den Schutz der europäischen Bürger vor digitalen Risiken durch ausländische Fahrzeug- und Gerätehersteller zu verbessern?*
29. *Welche Rolle spielen europäische Institutionen, etwa die Europäische Agentur für Cybersicherheit (ENISA), bei der Entwicklung und Überwachung von Sicherheitsstandards für digital vernetzte Fahrzeuge?*

30. *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?*

Diese Fragen sind kein Gegenstand meiner Vollziehung.

Zu Frage 9:

9. *Welche Vorgaben bestehen für Anbieter von digitalen Diensten und Fahrzeugen, um einen Zugriff Dritter auf Fahrzeugdaten, Standortinformationen, Kommunikations- und Nutzungsdaten zu verhindern?*

Anbieter von digitalen Diensten und Fahrzeugen sind verpflichtet rechtliche Vorgaben aus DSGVO, ePrivacy, NIS-2-Vorgaben und dem Data Act einzuhalten und haben technische, organisatorische und auch vertragliche Maßnahmen einzuhalten. Sie müssen gewährleisten, dass der unbefugte Zugriff Dritter auf Fahrzeug-, Standort-, Kommunikations- und weiterer Nutzungsdaten Dritter nicht erfolgen kann. Der Data Act regelt ebenfalls den Zugriff Dritter auf Produkt- und verbundene Dienstdaten. Diese Daten dürfen Dritte jedoch nur erhalten, wenn der Datennutzer seine Einwilligung gegeben hat.

Konkret gibt der Data Act außerdem vor, dass Anbieter von Datenverarbeitungsdiensten alle angemessenen technischen, organisatorischen und rechtlichen Maßnahmen (z.B. Vertragsregelungen) ergreifen müssen, um den staatlichen Zugang zu und die staatliche Übermittlung von in der Union gespeicherten nicht-personenbezogenen Daten im internationalen Umfeld und durch Drittländer zu verhindern. Die damit in Zusammenhang zu sehenden Mustervertragsklauseln der Europäischen Kommission enthalten strukturierte Vorgaben zu Zugriffsrechten, Nutzungsumfang, technischen und organisatorischen Maßnahmen, Geheimnisschutz, Haftung, Audit-Rechte sowie die Abgrenzung von personenbezogenen und nicht-personenbezogenen Daten.

Zu Frage 13:

13. *Wie stellt die Bundesregierung sicher, dass Bürger umfassend und transparent über die Datenerhebung, Datenverwendung und ihre Rechte durch Fahrzeughersteller und App-Anbieter informiert werden?*

Die Fahrzeughersteller und App-Anbieter sind gesetzlich dazu verpflichtet (DSGVO bei personenbezogenen Daten, Data Act), den Datennutzern umfassende Informationen sowie

klare und leicht zugängliche Kommunikationsformate bereitzustellen. Mit dem Data Act wird sichergestellt, dass die Datennutzer mehr Kontrollrechte über ihre Daten erhalten und die Aufsichtsbehörden Leitlinien, Informationsvorgaben und weitere Maßnahmen zur Orientierung zur Verfügung stellen.

Zu Frage 15:

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?

Mit dem „Digital Austria Act 2.0“ und dem Bekenntnis zur (nationalen und europäischen) digitalen Souveränität wird ein Rahmen geschaffen, welcher souveräne Cloud-Strukturen, staatliche IT, offene Standards und eine starke Ausrichtung auf europäische (Sicherheits-)Lösungen vorsieht. Hier wird im Hinblick auf Fahrzeugdaten eine souveräne und sichere kritische Infrastruktur vorangetrieben.

Dr. Christian Stocker

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2026-01-19T17:16:09+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-01-20T07:54:38+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	