3424/AB
vom 16.01.2026 zu 3932/J (XXVIII. GP)

Bundesministerium
Arbeit, Soziales, Gesundheit,
Pflege und Konsumentenschutz

sozialministerium.gv.at

Korinna Schumann
Bundesministerin

Herrn
Dr. Walter Rosenkranz
Präsident des Nationalrates
Parlament
1017 Wien

Geschäftszahl: 2025-0.982.954

Wien, 12.1.2026

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 3932/J der Abgeordneten Mag.a Marie-Christine Giuliani-Sterrer betreffend Gefahr für Datenschutz und nationale Sicherheit durch digitale Fahrzeuge** wie folgt:

Fragen 1 bis 30:

- *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?*

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

- *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?*
- *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?

Generell ist anzumerken, dass die Fragen ganz überwiegend nicht in den Zuständigkeitsbereich des Bundesministeriums für Soziales, Gesundheit, Pflege und Konsumentenschutz (BMASGPK) fallen. Das gilt insbesondere auch für die Verfolgung allfälliger datenschutzrechtlicher Verstöße.

Soweit die Zuständigkeit des BMASGPK konkret betroffen ist, kann ich das Folgende ausführen: Die Beschaffungsabteilungen der Ministerien sind gesetzlich verpflichtet, ihre Beschaffungen über die Bundesbeschaffung GmbH (BBG) abzuwickeln. Die BBG ist daher dafür zuständig, die Rahmenverträge rechtlich und technisch korrekt auszuschreiben und die Bestbieter auszuwählen. Im Ressort werden KFZ jedenfalls über bestehende BBG-Rahmenverträge beschafft bzw. daraus abgerufen.

Allgemein ist darauf hinzuwiesen, dass für den Bereich der digitalen Systeme bzw. digitaler Endgeräte generell immer die rechtlich definierten Mindeststandards (bspw. DSGVO, NIS-2 etc.) gelten.

Abschließend darf ich ergänzend auf die Beantwortung der Anfrage Nr. 3925/J durch den Bundesminister für Innovation, Mobilität und Infrastruktur verweisen.

Mit freundlichen Grüßen

Korinna Schumann

REPUBLIK ÖSTERREICH BUNDESMINISTERIUM FÜR ARBEIT, SOZIALES, GESUNDHEIT, PFLEGE UND KONSUMENTENSCHUTZ @ AMTSSIGNATUR	Unterzeichner	Bundesministerium für Arbeit, Soziales, Gesundheit, Pflege und Konsumentenschutz
	Datum/Zeit	2026-01-16T09:37:25+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.	1088205675
Hinweis	Dieses Dokument wurde amtssigniert.	
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.sozialministerium.at/site/Ministerium/Willkommen_im_Ministerium/Amtssignatur/Amtssignatur	

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2026-01-16T09:43:35+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	