

20.10.26

In - EU - Wi

**Antrag
des Freistaates Bayern**

Entschlieung des Bundesrates "Private Betreiber kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen strken: Videoberwachung rechtssicher ermglichen"

Der Bayerische Ministerprsident

Mnchen, 20. Oktober 2026

An den
Prsidenten des Bundesrates
Herrn Brgermeister
Dr. Andreas Bovenschulte

Sehr geehrter Herr Prsident,

gem dem Beschluss der Bayerischen Staatsregierung wird die als Anlage beigefgte

Entschlieung des Bundesrates „Private Betreiber kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen strken: Videoberwachung rechtssicher ermglichen“

mit dem Antrag bermittelt, dass der Bundesrat diese fassen mge.

Es wird gebeten, die Vorlage den zustndigen Ausschssen zur Beratung zuzuweisen.

Mit freundlichen Gren
Dr. Markus Sder

EntschlieÙung des Bundesrates „Private Betreiber kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen stärken: Videoüberwachung rechtssicher ermöglichen“

Der Bundesrat möge folgende EntschlieÙung fassen:

1. Der Bundesrat sieht angesichts der grundlegend veränderten Sicherheitslage eine Schutzlücke bei der Videoüberwachung kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen durch private Betreiber (einschließlich der Überwachung durch unbewegte Bilder). Drohnenüberflüge, Sabotageakte und hybride Angriffe sind keine abstrakten Szenarien mehr. Die Verwundbarkeit kritischer Infrastruktur wird ausgenutzt. Stromnetze, Wasserwerke, Flughäfen, Rechenzentren und Rüstungsbetriebe sind mögliche Ziele. Kritische Infrastruktur, verteidigungsrelevante Unternehmen und sonstige sicherheitsrelevante Anlagen sind auch dort ein Schutzgut von nationalem Rang, wo sie privat betrieben werden. Private Betreiber dieser Einrichtungen sind dabei keine beliebigen Datenverarbeiter, sondern verantwortliche Träger sicherheitsrelevanter Versorgungsfunktionen und tragen zur Verteidigungsfähigkeit und Sicherheit von Bund und Ländern bei. Dieser besonderen Stellung muss das Datenschutzrecht durch klare Befugnisse und einen angemessenen Vertrauensvorschuss Rechnung tragen.
2. Wirksamer Schutz beginnt dabei bereits vor dem Zaun: Wer erst filmt, wenn der Täter auf dem Gelände ist, handelt zu spät. Gerade Umspannwerke, Wasserwerke, Leitstellen, Flughäfen oder sicherheitsrelevante Produktionsstätten brauchen Kameras an ihren Zugängen und Werksgrenzen. Nur dann können Angriffe von außen (Drohnen, selbstgebaute Raketen etc.) wirksam erkannt und abgeschreckt werden. Es bedarf daher einer Ausweitung der per Video überwachbaren Bereiche auf das Vorfeld solcher Unternehmen, Betrieben und Einrichtungen.
3. Die durch Videoüberwachung erlangten Daten müssen so lange aufbewahrt werden können, dass sie im Falle eines Angriffs auch KI-gestützt für einen hinreichend weit zurückreichenden Zeitraum ausgewertet werden können. Eine Pflicht zur Kennzeichnung dieser Videoüberwachung sowie etwaige Auskunftsrechte zum gesammelten Material müssen entfallen, wo ein berechtigtes Interesse besteht, das bestehende Schutzbedürfnis geheim zu halten.
4. Die maßgebliche Stellschraube liegt im Bundesrecht. § 4 des Bundesdatenschutzgesetzes muss so weiterentwickelt werden, dass er privaten Betreibern kritischer Infrastruktur, verteidigungsrelevanter oder sonstiger sicherheitsrelevanter Unternehmen, die insoweit den Schutz ihrer Anlagen auch im öffentlichen Interesse wahrnehmen, rechtssicher ermöglicht, ihre Aufgabe durch Videokameras sowie nicht ortsgebundene Einrichtungen deutlich auszubauen, damit die Funktionsfähigkeit ihrer Einrichtungen gewährleistet wird. Die Spielräume der Datenschutz-Grundverordnung sind dazu auch im Lichte der gegenüber ihrem Erlass massiv zugespitzten Sicherheitslage auszudeuten und auszuschöpfen.

5. Der Bundesrat fordert deshalb die Bundesregierung auf, die Vorgaben des Bundesdatenschutzgesetzes in den folgenden Punkten weiterzuentwickeln:

- Die Videoüberwachung auch öffentlich zugänglicher Räume durch Betreiber kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen soll ausdrücklich bis zu 50 Meter vor der Grenze der Anlage zulässig sein. Der Schutz solcher Anlagen muss im Rahmen der Erforderlichkeit bzw. Datenminimierung auch im Lichte der Notwendigkeit von Resilienz-Maßnahmen zum Schutz solcher Einrichtungen über die konkrete Grundstücksgrenze hinaus in den öffentlichen Raum erstreckt werden können. So verpflichtet etwa § 13 des KRITIS-Dachgesetzes bestimmte Betreiber kritischer Anlagen ausdrücklich zu Resilienz-Maßnahmen, was das öffentliche Interesse am Selbstschutz kritischer Infrastruktur in privater Hand nochmals besonders unterstreicht. Dies soll insbesondere die Beobachtung von Zugängen, Werksgrenzen und gefährdeten Vorfeldbereichen erfassen.
- Die weitere, zweckändernde Verarbeitung und Nutzung der erhobenen Daten soll auch zur Aufklärung von Drohnenüberflügen, Sabotagehandlungen, Ausspähversuchen und sonstigen Sicherheitsvorfällen zulässig sein. Zu diesem Zweck sind die relevanten Daten den Sicherheitsbehörden des Bundes und der Länder im Bedarfsfall unverzüglich herauszugeben.
- Die Löschungsregelung soll eine Speicherdauer von bis zu einem Jahr ermöglichen.
- Besonderer Anpassungsbedarf besteht bei den Betroffenenrechten: Bei den genannten Unternehmen und Einrichtungen können Hinweise auf Videoüberwachung sowie Auskunftsrechte über gesammeltes Material den Schutz der Anlage schwächen. Sie können Kamerastandorte, Sicherheitsbereiche und sensible Zugänge offenlegen. Hier ist eine Ausnahme von der Kennzeichnungspflicht sowie von Auskunfts- und Widerspruchsrechten geboten.
- Der Einsatz von KI sollte explizit und umfassend ermöglicht werden. KI-Entwicklung und -nutzung können insofern im Rahmen smarterer Technologien ggf. auch zur Datenminimierung beitragen und damit grundrechtsschonend wirken.

6. Der Bundesrat hält es darüber hinaus für wünschenswert, auch auf Ebene der Datenschutz-Grundverordnung eine klarstellende Regelung für den Schutz kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen zu erreichen und das europäische Recht entsprechend zu ändern. Dies darf ein kurzfristiges Tätigwerden des nationalen Gesetzgebers im Rahmen der Auslegung der bestehenden Datenschutz-Grundverordnung jedoch nicht hemmen.

7. Die unabhängigen Datenschutzbehörden in Bund und Ländern sind aufgerufen, ihren Teil zum Schutz dieser Unternehmen, Betriebe und Einrichtungen beizutragen und die Güterabwägungen, die ihren bestehenden Leitlinien und Verlautbarungen zum Einsatz von Videokameras sowie nicht ortsgebundenen Einrichtungen durch private Betreiber kritischer Infrastruktur, verteidigungsrelevanter Unternehmen und sonstiger sicherheitsrelevanter Anlagen zugrunde liegen, unter Berücksichtigung der grundlegend veränderten Sicherheitslage zu überprüfen und anfragende Unternehmen zielgenau zu beraten.
8. Die Bundesregierung wird gebeten, dem Bundesrat binnen drei Monaten über die Ergebnisse der Prüfungen und die eingeleiteten gesetzgeberischen Maßnahmen zu berichten.