

**Anfrage zur schriftlichen Beantwortung E-001342/2024  
an die Kommission**

Artikel 138 der Geschäftsordnung

**Emmanuel Maurel** (The Left), **Geoffroy Didier** (PPE), **Patrick Breyer** (Verts/ALE), **Pierre Larroutou** (S&D)

**Betrifft:** Schutz der strategisch wichtigsten und sensibelsten europäischen Daten vor extraterritorialen ausländischen Gesetzen

Im Rahmen des europäischen Cloud-Zertifizierungssystems sollen die europäischen Anforderungen in Bezug auf die Sicherheit personenbezogener Daten harmonisiert werden.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) schlug bei der Datenspeicherung ursprünglich drei Risikostufen vor: „niedrig“, „erheblich“ und „hoch“. Die Risikostufe „hoch“ galt für die sensibelsten Daten (in den Bereichen Verteidigung, Gesundheit usw.) und bedeutete, dass die Daten in Europa gespeichert werden mussten. Bei der Risikostufe „hoch“ wurde von außereuropäischen Unternehmen (Amazon, Apple, Google usw.) zudem verlangt, Gemeinschaftsunternehmen mit europäischen Anbietern (OVH, Thalès usw.) einzurichten.

Auf diese Weise hätte sichergestellt werden sollen, dass Daten aus der EU in geeigneter Weise vor in den USA und China angewandten extraterritorialen Gesetzen (Cloud Act bzw. chinesisches Nachrichtendienstgesetz) geschützt würden, denen zufolge diese Regierungen aus Gründen der „nationalen Sicherheit“ ermächtigt werden, solche Daten zu kopieren, ganz unabhängig davon, wo sie gespeichert sind.

Der Fachpresse war jedoch Anfang April 2024 zu entnehmen, dass diese Empfehlungen aus dem aktuellen Arbeitsplan der ENISA verschwunden sind. Wichtige digitale Akteure in Europa haben in einem Schreiben an die Kommission zu Recht Bedenken geäußert.

1. Unterstützt die Kommission die Streichung dieser Empfehlungen?
2. Wie gedenkt sie, die sensibelsten Daten vor extraterritorialen ausländischen Gesetzen zu schützen?

Eingang:25.4.2024