

Fraktionen im Rat der Stadt - 52062 Aachen

Oberbürgermeister
Dr. Michael Ziemons
Rathaus/Markt
52058 Aachen

Geschäftsstellen

Verwaltungsgebäude Katschhof
Johannes-Paul-II.-Straße 1
52062 Aachen

Grüne 0241 / 432 -7217

Antrag Nr. 2026_19

LINKE 0241 / 432 -7244

Aachen, 11.09.2026

Ratsantrag

Einführung eines Souveränitätschecks für die städtische IT- und Softwarebeschaffung

Sehr geehrter Herr Oberbürgermeister,

die Fraktionen von Bündnis 90/Die GRÜNEN und die Linke beantragen, im Rat der Stadt Aachen folgenden Beschluss zu fassen:

Der Rat der Stadt Aachen möge beschließen:

1. Die Verwaltung wird beauftragt, für zukünftige Beschaffungen von Software und IT-Dienstleistungen einen **Souveränitätscheck** einzuführen. Dieser Check ist verpflichtender Bestandteil des Beschaffungsprozesses und dient der systematischen Bewertung digitaler Souveränität vor jeder Vergabeentscheidung.
2. Die Verwaltung wird beauftragt, dem Rat **verbindliche Kriterien** vorzulegen, anhand derer die digitale Souveränität einer Software bewertet wird. Diese Kriterien sollen sich insbesondere auf folgende Dimensionen beziehen:

- **Selbstständigkeit** (u. a. Unabhängigkeit von einzelnen Anbietern, Vermeidung von Lock-in-Effekten, Wechselmöglichkeiten zu alternativen Lösungen)
 - **Selbstbestimmtheit** (u. a. Kontrolle über Daten und Prozesse, Einsatz offener Standards und Schnittstellen, Einflussmöglichkeiten auf die Weiterentwicklung der Software)
 - **Sicherheit** (u. a. Transparenz über Datenverarbeitung, Schutz vor externem Zugriff und Manipulation, Robustheit gegenüber geopolitischen Risiken)
3. Die Verwaltung wird beauftragt, klar zu definieren, **ab welchem Bewertungsergebnis eine Software nicht mehr für eine Beschaffung in Frage kommt** bzw. unter welchen Voraussetzungen von einer Beschaffung Abstand genommen werden muss oder zumindest eine vertiefte Risikoprüfung sowie die Prüfung von Alternativen und Umstiegsszenarien erforderlich ist.
4. Bei der Ausgestaltung von Kriterienkatalog und Schwellenwerten orientiert sich die Verwaltung an dem von der Landeshauptstadt München entwickelten Vorgehen (Souveränitätscheck des IT-Referats München,¹ vgl. Sitzungsvorlage² Nr. 20-26 / V 18562) und den Kriterien für Digitale Souveränität³ des Zentrums für Digitale Souveränität (ZenDiS).⁴
5. Die Verwaltung legt dem Ausschuss für Digitalisierung zu jeder Neubeschaffung die Ergebnisse des Souveränitätschecks vor.

Begründung

Die digitale Souveränität von Kommunen gewinnt angesichts wachsender Abhängigkeiten von einzelnen, häufig außereuropäischen Softwareanbietern zunehmend an Bedeutung. Eine stabil funktionierende Verwaltungs-IT gehört mittlerweile zur kritischen Infrastruktur einer Stadt. Abhängigkeiten von Anbietern, die außerhalb europäischer Rechtsräume agieren, bergen erhebliche Risiken: von der Abschöpfung sensibler Daten über erpresserischen Druck bis hin zu Abschaltungen oder Störungen zentraler Dienste, etwa durch geopolitische Entwicklungen, veränderte Lizenzbedingungen oder politische Entscheidungen im Sitzstaat des Anbieters.

Diese Bedrohungsszenarien sind längst nicht mehr rein theoretischer Natur, sondern haben sich in der jüngeren Vergangenheit bereits konkret realisiert. So wurde der Chefankläger des

¹ <https://muenchen.digital/projekte/digitale-souver%C3%A4nit%C3%A4t.html>

² <https://risi.muenchen.de/risi/dokument/v/9509022>

³ <https://souveraenitaetscheck.de/>

⁴ <https://www.zendis.de/>

Internationalen Strafgerichtshofs infolge US-Sanktionen von der Nutzung US-amerikanischer Softwareprodukte wie Microsoft-Diensten ausgeschlossen⁵. In einem anderen Fall musste Microsoft aufgrund des US-amerikanischen Cloud Acts Gesprächsprotokolle und weitere Daten niederländischer Verwaltungsangestellter an US-Behörden herausgeben⁶. Beide Fälle zeigen exemplarisch, dass der Einsatz nicht-souveräner Software auch europäische bzw. internationale Institutionen und deren Beschäftigte unmittelbar und mit weitreichenden Konsequenzen betreffen kann, unabhängig davon, ob ein konkreter Anlass für eine Sanktion oder einen Datenzugriff vorliegt.

Die Stadt Aachen sollte diesen Risiken proaktiv begegnen, statt erst im Ernstfall zu reagieren. Ein strukturierter Souveränitätscheck stellt sicher, dass Fragen der Unabhängigkeit, der Kontrolle über eigene Daten und Prozesse sowie der IT-Sicherheit bereits vor einer Beschaffungsentscheidung systematisch mitgedacht werden und nicht erst, wenn eine problematische Abhängigkeit bereits entstanden ist.

Sowohl die Stadt München als auch das ZenDiS haben hierzu bereits wichtige Vorarbeit geleistet: Beide orientieren sich dabei an den drei Kernbegriffen Selbstständigkeit, Selbstbestimmtheit und Sicherheit. Die Stadt München leitet daraus auch konkrete Bewertungskriterien sowie Konsequenzen für die Beschaffung ab.

Es ist naheliegend und ressourcenschonend, dass sich Aachen an diesem bereits dokumentierten Vorgehen orientiert, statt eine eigene Methodik von Grund auf neu zu entwickeln. Durch eine Anpassung des Münchner Modells an die Aachener Gegebenheiten kann die Stadt schnell und mit vertretbarem Aufwand ein wirksames Instrument etablieren, um zukünftige Softwarebeschaffungen nachhaltiger, sicherer und unabhängiger zu gestalten.

Ein klar definierter Kriterienkatalog schafft zudem Transparenz und Rechtssicherheit für Vergabeentscheidungen: Sowohl die Verwaltung als auch der Rat erhalten eine verlässliche Grundlage, um zu beurteilen, wann eine Software als digital souverän gelten kann und wann eine Beschaffung kritisch zu hinterfragen oder abzulehnen ist. Etwa aufgrund mangelnder Wechsellmöglichkeiten oder unzureichender Kontrolle über Daten. Damit leistet Aachen einen wichtigen Beitrag zur Zukunftssicherheit und Resilienz der eigenen digitalen Infrastruktur.

Mit freundlichen Grüßen

Carsten Schaadt
Fraktionssprecher Grüne

Philipp Heyken-Soares
Digitalpolitischer Sprecher Grüne

Andreas Nositschka
Fraktionssprecher die Linke

Sebastian Günther
Digitalpolitischer Sprecher die Linke

⁵ <https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3>

⁶ <https://www.itmagazine.ch/artikel/87259/Cloud-Act-in-Aktion-Microsoft-haendigt-Daten-von-Beamten-an-USA-aus.html>