Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern

PRESSEMITTEILUNG

Schwerin, den 11. April 2025

LfDI MV warnt öffentliche Stellen vor Cloud Computing mit Anbietern aus Drittländern

Vielerorts laufen demnächst in den Kommunen sogenannte On-Premise-Lösungen aus. Große proprietäre Hersteller verabschieden sich von diesem Lizenzmodell und setzen weitestgehend auf Cloud-Computing bzw. Software as a Service, nicht selten verbunden mit Abo-Modellen. Sebastian Schmidt, der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV) rät öffentlichen Stellen, bei der Umstellung verstärkt auf Open Source-Produkte zu setzen.

Bei On-Premise-Lizenzmodellen betreiben die Kommunen ihre Anwendungen als lokale Lösungen auf den eigenen Servern. Unabhängig davon, wer die Komponenten oder Programme herstellt, mit denen die Daten der Bürgerinnen und Bürgern verarbeitet werden, bleiben diese in der Obhut der Kommune. Bei Cloud Computing hingegen werden Anwendungen über das Internet zur Verfügung gestellt und personenbezogene Daten in der Cloud verarbeitet. Das ist prinzipiell datenschutzrechtlich nicht zu beanstanden, solange die Kommune die vollständige Kontrolle über die Daten der Bürgerinnen und Bürgern behält. Bei Anbietern, die ihren Hauptsitz in Ländern außerhalb der europäischen Union haben, ist dies jedoch kaum noch sicherzustellen. Selbst wenn die Anbieter vertraglich zusichern, sich an europäisches Datenschutzrecht zu halten, können rechtliche Bestimmungen des jeweiligen Drittlands diese dazu verpflichten, Daten an die Sicherheitsbehörden des Drittlandes herauszugeben. Wenn zudem faktisch die Möglichkeit besteht, aus dem Drittland auf die Datenverarbeitung an sich Einfluss zu nehmen und Systeme einfach vom Netz zu nehmen, begeben sich öffentlichen Stellen in völlige Abhängigkeit.

„Es geht um weit mehr, als um die Frage, ob ein ausländischer Geheimdienst personenbezogene oder vertrauliche Daten zur Kenntnis nehmen kann. Es geht angesichts der derzeitig unsicheren geopolitischen Lage um die Funktionsfähigkeit des Staates.“, appelliert Schmidt. Sind Daten in den Kommunen plötzlich nicht mehr verfügbar, können grundlegende staatliche Leistungen nicht sichergestellt werden. „Das schwächt das Vertrauen der Bürgerinnen und Bürger in den Staat – aber auch die lokale Wirtschaft.“, mahnt Schmidt. Zudem nutzen Anbieter ihre Marktmacht nicht selten, um sich Nutzungsrechte an den verarbeiteten Daten einzuräumen, beispielsweise zur Produktverbesserung oder zum Training künstlicher Intelligenz. Für Daten, die der Staat von Bürgerinnen und Bürgern verarbeitet, fehlt es dazu aber an jeglicher Rechtsgrundlage. Schmidt appelliert daher an die Verwaltung, sich bei der Digitalisierung unabhängig von Anbietern aus Drittstaaten zu machen.

Ähnlich äußerten sich Abgeordnete in der gestrigen Aussprache im Landtag Mecklenburg-Vorpommern zum Thema digitale Souveränität. Sebastian Schmidt begrüßt das parteiübergreifende Bekenntnis zu mehr digitaler Unabhängigkeit, wie sie beispielsweise in Schleswig-Holstein gelebt wird. Auch der Landesrechnungshof plädiert seit Jahren für die Nutzung von Open-Source-Produkten, deren Quellcode öffentlich ist und den individuellen Bedürfnissen angepasst werden kann. Neben einer Stärkung der digitalen Souveränität sinken in der Regel auf lange Sicht auch die Anschaffungs- und Wartungskosten, zudem wird die heimische Wirtschaft gestärkt, wenn derartige Leistungen lokal beauftragt werden. Schließlich können mit Open-Source-Produkten oder europäischen Anbietern Rechtsunsicherheiten umgangen werden. Der Europäische Gerichtshof hat seit 2016 zwei Angemessenheitsbeschlüsse für die Übermittlung personenbezogener Daten in die USA für ungültig erklärt. In der Konsequenz waren viele Datenübermittlungen in die USA plötzlich unzulässig. Öffentliche Stellen können vor dem Hintergrund knapper finanzieller und personeller Ressourcen sowie strenger Vorschriften, beispielsweise bei der Vergabe, jedoch oftmals nicht in der gebotenen Schnelligkeit auf eine veränderte Rechtslage reagieren. Neben Maßnahmen der Datenschutzaufsichtsbehörden drohen dann vor allem Schadensersatzansprüche von Bürgerinnen und Bürgern, wenn weiterhin rechtswidrig Daten verarbeitet werden. „Wer jetzt seine Anwendungen und Systeme umstellt, sollte daher genau abwägen, was auch langfristig rechtssicher in der Kommune zum Einsatz kommen kann.“, rät Schmidt abschließend.

Kontakt: presse@datenschutz-mv.de