

Anfrage der Ratsfraktion Die Linke vom 21.08.2026:
Sicherheit der kommunalen Bürger*innendaten bei der Nutzung von Software aus Nicht-EU-Staaten

Frage 1:

Welche technischen, organisatorischen und vertraglichen Zusatzmaßnahmen (z. B. eigene Verschlüsselung mit exklusiver Schlüsselgewalt, Deaktivierung intransparenter Hintergrunddienste, Unterbindung des Abflusses von Telemetriedaten) hat die städtische IT-Abteilung (bzw. ITK-Rheinland) vorgenommen, um den strengen datenschutzrechtlichen Kernforderungen der Datenschutzkonferenz (DSK) und den Erkenntnissen des EDSB-Verfahrens beim Einsatz von Microsoft-Produkten (Windows, Microsoft 365, Teams) in der Düsseldorfer Stadtverwaltung vollumfänglich gerecht zu werden?

Antwort:

Die Landeshauptstadt Düsseldorf und die ITK Rheinland setzen Microsoft-Produkte verantwortungsvoll und unter Beachtung der jeweils geltenden datenschutzrechtlichen Anforderungen ein. Ziel ist es, die für eine leistungsfähige Verwaltung erforderlichen Anwendungen bereitzustellen und zugleich die Verarbeitung personenbezogener Daten auf das notwendige Maß zu begrenzen.

Die häufig zitierte Bewertung der Datenschutzkonferenz (DSK) aus dem Jahr 2022 bezog sich insbesondere auf die damals geltenden Vertragsbedingungen von Microsoft. Diese wurden inzwischen überarbeitet. Eine aktuelle, allgemeinverbindliche Handreichung der DSK oder der nordrhein-westfälischen Datenschutzaufsicht zum Einsatz von Microsoft 365 liegt bislang nicht vor.

Auch das Verfahren des Europäischen Datenschutzbeauftragten zum Einsatz von Microsoft 365 durch die EU-Kommission wurde nach vorgenommenen Nachbesserungen eingestellt. Für mögliche Datenübermittlungen in die USA besteht derzeit mit dem EU-U.S. Data Privacy Framework zudem eine gültige rechtliche Grundlage.

Unabhängig davon werden die eingesetzten Microsoft-Produkte fortlaufend geprüft und datenschutzgerecht konfiguriert. Nicht benötigte Funktionen und Datenübermittlungen werden soweit wie möglich eingeschränkt. Komponenten werden nur dann freigeschaltet, wenn sie für einen sicheren, zuverlässigen und ordnungsgemäßen Betrieb erforderlich sind. Dabei werden sowohl technische und organisatorische Schutzmaßnahmen als auch die jeweils geltenden vertraglichen und rechtlichen Rahmenbedingungen berücksichtigt. Die LHD und die ITK Rheinland beobachten die weitere rechtliche und technische Entwicklung kontinuierlich und passen den Einsatz der Produkte bei Bedarf an. So wird sichergestellt, dass die Verwaltung arbeitsfähig bleibt und zugleich ein möglichst hohes Datenschutzniveau gewährleistet wird.

Frage 2:

Ist die Stadtverwaltung, die ITK-Rheinland haftbar oder wer trägt im Falle einer rechtswidrigen Datenübermittlung in Drittstaaten (z. B. unbefugte Datenzugriffe unter dem US Cloud Act) oder bei einem sonstigen datenschutzrechtlichen Schadensfall das rechtliche und finanzielle Haftungsrisiko (inklusive potenzieller Schadensersatzforderungen betroffener Bürger gemäß Art. 82 DSGVO)?

Antwort:

Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist als Behörde die Landeshauptstadt Düsseldorf – Der Oberbürgermeister. Sie trägt grundsätzlich die rechtliche Verantwortung für die datenschutzkonforme Verarbeitung personenbezogener Daten. Das gilt auch dann, wenn personenbezogene Daten bei externen IT-Dienstleistern oder dem Zweckverband ITK-Rheinland im Auftrag verarbeitet werden.

Da eine Person, der wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, nach Art. 82 Abs. 1 DSGVO Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter geltend machen kann, tragen grundsätzlich beide ein Haftungsrisiko bei nicht DSGVO-konformer Datenverarbeitung wie z.B. einer rechtswidrigen Drittstaatenübermittlung personenbezogener Daten.

Der Dienstleister agiert im Regelfall als Auftragsverarbeiter gem. Art. 4 Nr. 8 DSGVO. Er haftet gegenüber betroffenen Personen gemäß Art. 82 Abs. 2 Satz 2 DSGVO nur dann, wenn er spezifische Pflichten der DSGVO verletzt hat, die sich ausdrücklich an Auftragsverarbeiter richten, oder wenn er entgegen rechtmäßigen Weisungen der Stadt gehandelt hat, z. B. bei einer Verletzung vereinbarter Sicherheitsstandards.

Liegt eine Haftung beider Parteien vor, haften die Stadt und der Auftragsverarbeiter gegenüber der geschädigten Person gem. Art. 82 Abs. 4 DSGVO als Gesamtschuldner.

Frage 3:

Welche Notfallpläne und langfristigen Migrationsstrategien verfolgt die Verwaltung, um den Schutz sensibler Bürgerdaten unabhängig von US-amerikanischen Cloud-Anbietern zu gewährleisten?

Antwort:

Die Verwaltung der Stadt Düsseldorf setzt jede Software derzeit datenschutzkonform ein. Für jede Anwendung wird geprüft, dass die Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) sowie die spezifischen Regelungen des NRW-Landes-Datenschutzgesetzes erfüllt sind.

Die Entwicklung und Weiterentwicklung dieser Softwarelandschaft wird engmaschig überwacht. Insbesondere werden gesetzliche Veränderungen durch die US-Regierung im Auge behalten. Geprüft wird fortlaufend:

- Sicherheits- und Datenschutz-Updates der eingesetzten Produkte.
- Compliance-Reports von den Anbietern sowie interne Audits.
- Risiko-Bewertungen bei neuen Features oder bei Änderungen in den gesetzlichen Vorgaben.

Durch diese kontinuierliche Beobachtung kann die Landeshauptstadt Düsseldorf zeitnah reagieren, wenn Anpassungen, Patches oder alternative Lösungen notwendig werden. Strategisch wird eine Ablösung von US-amerikanischen Anbietern stets mit eruiert.