Der Bayerische Landesbeauftragte
für den Datenschutz

Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen

Aktuelle Kurz-Information 39

Stichwörter: Angemessenheitsbeschluss – Datenschutz-Sicherheitskonzept – Drittland – Drittlandtransfer – Inhaltsdaten – Office-Anwendungen – Pseudonymisierung – Schlüssel – Standarddatenschutzklauseln – Verschlüsselung – Videokonferenz-Systeme – Zuordnungsregel | **Stand:** 1. Dezember 2021

Gegenwärtig bestehen bei zahlreichen bayerischen öffentlichen Stellen (Verantwortliche) Unsicherheiten, was den Einsatz von Office-Anwendungen aus dem Nicht-EU-Ausland, insbesondere den Vereinigten Staaten von Amerika (USA), betrifft. Den Bayerischen Landesbeauftragten für den Datenschutz haben insoweit zahlreiche Anfragen vor allem aus dem Bereich der bayerischen öffentlichen Schulen erreicht. Die Nutzung solcher Produkte bringt oftmals eine Übermittlung personenbezogener Daten in ein Drittland mit sich; Übermittlungen dieser Art sind seit Geltungsbeginn der Datenschutz-Grundverordnung allerdings strikt reglementiert (siehe im Einzelnen Art. 44 Datenschutz-Grundverordnung – DSGVO). 1

Die vorliegende Aktuelle Kurz-Information erläutert nach einem Hinweis zum Datenschutz-Sicherheitskonzept (1.) zunächst die aktuell bestehenden rechtlichen Rahmenbedingungen für eine Übermittlung personenbezogener Daten in ein Drittland auf Grundlage der Art. 44 ff. DSGVO (2.). Sie zeigt ferner auf, welche Anforderungen an die Rechenschaftspflicht des Verantwortlichen zu stellen sind (3.). 2

Verantwortliche sollten berücksichtigen, dass sich die Rechtsprechung und die Positionen der Datenschutz-Aufsichtsbehörden zu Fragen der Art. 44 ff. DSGVO in zügiger Geschwindigkeit fortentwickeln. Daher sollte stets auf neue Entscheidungen und Veröffentlichungen geachtet werden. 3

1. Datenschutz-Sicherheitskonzept

Als eine **vorbereitende Maßnahme** sollte der Verantwortliche, der eine **Office-Anwendung aus einem Drittland** einsetzen möchte, stets ein **Datenschutz-Sicherheitskonzept** erstellen. Das Datenschutz-Sicherheitskonzept sollte insbesondere auf die folgenden Fragen eingehen: 4

- Welches **Produkt** soll in welcher **IT-Umgebung** eingesetzt werden?
- Welche **Kategorien personenbezogener** Daten sollen mit dem Produkt verarbeitet werden?
- Welche **nachteiligen Folgen** können sich daraus für die Vertraulichkeit, Verfügbarkeit und Integrität von personenbezogenen Daten ergeben? Wie sind diese Folgen und deren

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Eintrittswahrscheinlichkeiten zu **bewerten** und mit welchen Maßnahmen ist ihnen gegebenenfalls zu **begegnen**? Zur Beantwortung dieser Fragen kann zunächst auf den einschlägigen BSI-Standard[1] zurückgegriffen werden.

2. Übermittlung personenbezogener Daten auf Grundlage von Art. 44 ff. DSGVO

5 Soweit eine Office-Anwendung eingesetzt werden soll, bei deren Nutzung personenbezogene Daten von Beschäftigten sowie Bürgerinnen und Bürgern in einen Staat außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung übermittelt werden oder Stellen in einem solchen Staat eine Zugriffsmöglichkeit eröffnet wird, muss die Folgenbetrachtung auch die für solche Datentransfers einschlägigen gesetzlichen Vorgaben berücksichtigen. Die Bewertung nachteiliger Folgen für die Vertraulichkeit der personenbezogenen Daten wie auch die Implementierung von Maßnahmen zu ihrer Minimierung ist in diesem Fall durch Art. 44 ff. DSGVO angeleitet.

6 **Insbesondere** ist die **Zulässigkeit der Übermittlung von personenbezogenen Daten** in das Drittland an **Art. 44 ff. DSGVO** zu messen; die Vorschriften sollen sicherstellen, dass personenbezogene Daten nach Verlassen des Geltungsbereichs der Datenschutz-Grundverordnung nicht in eine Verarbeitungsumgebung mit (signifikant) geringerem Datenschutzniveau geraten.

7 Grundlage der Übermittlung kann ein die Vergleichbarkeit des Datenschutzniveaus verbindlich feststellender, wirksamer **Angemessenheitsbeschluss** der Europäischen Kommission sein (Art. 45 Abs. 1 DSGVO). Für die USA, wo zahlreiche Anbieter von Office-Anwendungen beheimatet sind, liegt ein Angemessenheitsbeschluss gegenwärtig allerdings nicht vor. Die in Rede stehenden Übermittlungen können regelmäßig auch nicht auf die Ausnahmetatbestände gestützt werden, die Art. 49 Abs. 1 DSGVO für bestimmte Fälle vorsieht.

8 Vor diesem Hintergrund ist die **Vergleichbarkeit des Datenschutzniveaus durch den Verantwortlichen und seinen Vertragspartner sicherzustellen**, der als Datenempfänger fungieren soll. Dazu müssen geeignete Garantien vorgesehen sein und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (Art. 46 Abs. 1 DSGVO). Vorliegend kommen hierzu insbesondere Regelungen in **Standarddatenschutzklauseln** in Betracht (Art. 46 Abs. 2 Buchst. c DSGVO). Ein entsprechendes aktuelles Klauselwerk hat die Europäische Kommission im Sommer 2021 bereitgestellt.[2]

9 Da das Klauselwerk grundsätzlich nicht die Heimatrechtsordnung des ausländischen Datenempfängers modifizieren kann, genügen der Verantwortliche und sein Vertragspartner jedoch den Anforderungen der Datenschutz-Grundverordnung **nicht** bereits dann, wenn sie die Geltung des Klauselwerks vereinbaren.[3]

10 Geeignete Garantien im Sinne von Art. 46 Abs. 1 DSGVO werden nur vermittelt, wenn das **Klauselwerk auch (tatsächlich) wirksam** ist. Dazu bedarf es einer Betrachtung der Heimatrechtsordnung des ausländischen Datenempfängers. Der Europäische Datenschutzausschuss hat für diese Betrachtung ausführliche Hinweise veröffentlicht.[4]

Soweit die Betrachtung der Heimatrechtsordnung des ausländischen Datenempfängers ergibt, dass das Klauselwerk dort nicht in vollem Umfang die beabsichtigte Wirkung zu entfalten vermag, ist eine **Kompensation durch zusätzliche Maßnahmen** zu prüfen.[5] Dazu kann auch eine **Verschlüsselung** und/oder **Pseudonymisierung** zählen.[6] Ist eine Kompensation nicht möglich, muss eine Übermittlung personenbezogener Daten an den ausländischen Datenempfänger unterbleiben. 11

Aus diesen grundsätzlichen Bemerkungen ergeben sich für den Einsatz konkreter Office-Anwendungen insbesondere die nachstehenden **Konsequenzen**: 12

– Ausgangspunkt aller Überlegungen sollte ein **Datenschutz-Sicherheitskonzept** sein, das eine datenschutzrechtliche Folgenbetrachtung vornimmt. 13

  Das Datenschutz-Sicherheitskonzept muss klare Aussagen darüber enthalten, welche **Kategorien personenbezogener Daten** von Beschäftigten sowie Bürgerinnen und Bürgern (in einer Schule etwa also von Schülerinnen, Schülern, Eltern, Lehrkräften und sonstigem Schulpersonal) in ein Drittland übermittelt werden oder Zugriffen von dort ausgesetzt werden sollen.

  Bei der **Folgenbetrachtung** ist für die konkrete Office-Anwendung insbesondere die nachteilige Folge zu würdigen, dass Behörden aus einem Drittland auf personenbezogene Daten von Beschäftigten sowie Bürgerinnen und Bürgern Zugriff nehmen könnten (auch im Wege einer Anforderung zur Offenlegung von personenbezogenen Daten). Diese nachteilige Folge ist bereits dann zu berücksichtigen, wenn die Rechtsordnung des Drittlandes zugunsten dortiger Behörden in Bezug auf die zu übermittelnden personenbezogenen Daten Zugriffsbefugnisse vorsieht, die aus unionsrechtlicher Perspektive als unverhältnismäßig erscheinen. Die nachteilige Folge kann grundsätzlich nicht allein durch eine Wahrscheinlichkeitsbetrachtung („bisher ist ja nichts passiert“) auf Grundlage von Angaben des Vertragspartners relativiert werden.

– Der Verantwortliche sollte das Rechtsverhältnis mit dem Vertragspartner in Ansehung von Datenübermittlungen in ein Drittland unter Einbezug der **aktuellen Standarddatenschutzklauseln** gestalten. 14

– Bei der Prüfung der **tatsächlichen Wirksamkeit des vereinbarten Klauselwerks** sind hinsichtlich des Drittlands USA zumindest diejenigen Vorgaben des US-amerikanischen Rechts zu berücksichtigen, die der Europäische Gerichtshof in seiner „Schrems II“-Entscheidung angesprochen hat.[7] 15

  Insofern dürfte nach der derzeitigen Auffassung des Bayerischen Landesbeauftragten für den Datenschutz die tatsächliche Wirksamkeit des vereinbarten Klauselwerks anzunehmen sein, wenn der Verantwortliche den Nachweis erbringt, dass die zu übermittelnden personenbezogenen Daten aus Rechtsgründen von vornherein nicht Gegenstand der betreffenden Zugriffsrechte US-amerikanischer Behörden werden können.

– Lässt sich dieser Nachweis nicht führen, ist als **Kompensation** eine Verschlüsselung und/oder Pseudonymisierung der personenbezogenen Daten in Betracht zu ziehen. Der 16

Verantwortliche muss in diesem Fall zudem den Nachweis erbringen, dass eine Aufhebung der Verschlüsselung und/oder Pseudonymisierung bei dem ausländischen Vertragspartner durch Behörden seines Heimatstaats ausgeschlossen werden kann.

Bei der Bewertung der nachteiligen Folge einer Aufhebung der Verschlüsselung und/oder Pseudonymisierung, die im Rahmen des Datenschutz-Sicherheitskonzepts durchgeführt werden kann, sollten nicht nur die Erfahrungen, die der ausländische Vertragspartner mit Zugriffsersuchen durch Behörden seines Heimatstaats gemacht hat, sondern auch alle weiteren verfügbaren Informationen[8] einbezogen werden. Entsprechendes gilt für die Bemessung kompensatorischer Maßnahmen, insbesondere für die Beantwortung der Frage, ob eine Verschlüsselung oder Pseudonymisierung ausreichend stark ist. Auch hier gilt (vgl. Rn. 13): Dass „bisher nichts passiert ist", bedeutet nicht, dass diese Maßnahmen vernachlässigt werden dürfen.

17 – Speziell beim Betrieb eines **Videokonferenz-Systems** fallen zumindest temporär Bild- und Tondateien an. Nach aktuellem Kenntnisstand ist eine ausreichend starke Verschlüsselung und/oder Pseudonymisierung insofern derzeit noch nicht möglich; dies gilt jedenfalls für typische Nutzungsszenarien im Schulbereich.

Datenschutzrechtliche Bedenken betreffend eine Übermittlung in das Drittland USA können hier auch nicht dadurch ausgeräumt werden, dass auf eine dauerhafte Aufzeichnung verzichtet wird und/oder die Dateien physikalisch im Geltungsbereich der Datenschutz-Grundverordnung gespeichert werden. US-amerikanische Anbieter sind als in den USA ansässige Unternehmen Zugriffsrechten US-amerikanischer Behörden ausgesetzt; dies gilt insbesondere für Regelungen des US CLOUD Act.[9] Entsprechenden Ersuchen kann allenfalls ausnahmsweise im Einklang mit der Datenschutz-Grundverordnung nachgekommen werden.[10] Im Übrigen ist zu bedenken, dass gegebenenfalls Verkehrsdaten übermittelt werden, bei denen ein Personenbezug hergestellt werden kann.

18 – Bei **anderen Office-Anwendungen** als Videokonferenz-Systemen kann eine ausreichend sicher gestaltete **Pseudonymisierung** insbesondere unter den folgenden Voraussetzungen in Betracht kommen:

(1) **Angemessen starke Pseudonymisierungsmethode:** Personenbezogene Daten werden so verarbeitet, dass sie ohne Hinzuziehung zusätzlicher Informationen weder einer spezifischen betroffenen Person zugeordnet noch dazu verwendet werden können, die betroffene Person in einer größeren Gruppe zu identifizieren. Zudem darf ein Abgleich mit sämtlichen Informationen, die Dritten zur Verfügung stehen, nicht dazu führen, dass die pseudonymisierten Daten identifizierten oder identifizierbaren natürlichen Personen zugeordnet werden können.

(2) **Besonderer Schutz der Zuordnungsregeln:** Die Zuordnung der pseudonymisierten Daten zu Identitätsinformationen („Zuordnungsregeln", z. B. Datentabelle oder Formel) und damit die Re-Identifizierung darf nur durch den Verantwortlichen (beispielsweise: die Schule) oder einen Auftragsverarbeiter, der als Vertrauensinstanz agiert und auf den die Datenschutz-Grundverordnung anwendbar ist, möglich sein. Zudem müssen die Zuordnungsregeln grundsätzlich innerhalb der EU

gehalten und einem angemessenen Schutz durch technische und organisatorische Maßnahmen gegen unbefugte Zugriffe, gegen unbefugte Veränderungen sowie gegen Störung der erforderlichen Verfügbarkeit unterliegen.

(3) **Stand der Technik:** Das eingesetzte Pseudonymisierungsverfahren muss grundsätzlich dem Stand der Technik entsprechen. Die Wirksamkeit der Pseudonymisierung als datenschutzrechtliche Schutzmaßnahme muss durch bedarfsgerechte Überprüfungen durchgängig gewährleistet sein.

– Entsprechend sind folgende Anforderungen an eine ausreichend sicher gestaltete **Verschlüsselung** zu stellen: 19

(1) **Angemessen starke Verschlüsselungsmethode:** Der Verschlüsselungsalgorithmus und seine Parametrisierung (z. B. Schlüssellänge, Verschlüsselungsstärke, Betriebsmodus) müssen angemessen sein und den spezifischen Zeitraum berücksichtigen, für den die Vertraulichkeit der verschlüsselten personenbezogenen Daten sicherzustellen ist.

(2) **Besonderer Schutz der Schlüssel:** Die Schlüssel müssen allein durch den Verantwortlichen (beispielsweise: die Schule) oder einen Auftragsverarbeiter, der als Vertrauensinstanz agiert und auf den die Datenschutz-Grundverordnung anwendbar ist, verwaltet und kontrolliert werden. Dadurch wird ein Zugriff auf unverschlüsselte Daten (Klardaten) durch unberechtigte Dritte mit Hilfe einer Ende-zu-Ende-Verschlüsselung ausgeschlossen. Zudem muss der Verschlüsselungsalgorithmus fehlerfrei durch ordnungsgemäß gepflegte Software implementiert sein, deren Konformität mit der Spezifikation des ausgewählten Algorithmus etwa durch Zertifizierung bestätigt wurde. Die Verschlüsselung muss – unter Berücksichtigung der zur Verfügung stehenden Ressourcen und technischen Möglichkeiten (z. B. Rechenleistung für Brute-Force-Angriffe) – Robustheit gegen eine eventuell durchgeführte Kryptoanalyse bieten. Ferner muss im Hinblick auf die Schlüssel, deren Generierung und Einsatz ein angemessener Schutz durch technische und organisatorische Maßnahmen gegen unbefugte Zugriffe, gegen unbefugte Veränderungen sowie gegen Störung der erforderlichen Verfügbarkeit bestehen.

(3) **Stand der Technik:** Das eingesetzte Verschlüsselungsverfahren muss grundsätzlich dem Stand der Technik entsprechen. Die Wirksamkeit der Verschlüsselung als datenschutzrechtliche Schutzmaßnahme muss durch bedarfsgerechte Überprüfungen durchgängig gewährleistet sein.

3. Rechenschaftspflicht

Verantwortliche trifft nach Art. 5 Abs. 2 DSGVO eine Rechenschaftspflicht. Die Rechenschaftspflicht bezieht sich auch auf den Verarbeitungsgrundsatz „Rechtmäßigkeit“ (Art. 5 Abs. 1 Buchst. a DSGVO). Sie gewährleistet, dass Verantwortliche ihre Überlegungen zu den rechtlichen Grundlagen einer Verarbeitung festhalten; für die Datenschutz-Aufsichtsbehörden werden diese Überlegungen so kontrollierbar. Im Rahmen der Rechenschaftspflicht 20

müssen Verantwortliche, die Datentransfers in Drittstaaten durchführen möchten, auch dokumentieren, dass sie die durch Art. 44 ff. DSGVO geforderte, unter Rn. 5 ff. näher erläuterte Prüfung vorgenommen haben. Diese gesetzlichen Anforderungen haben Anteil an dem Regelungsgefüge, das die Rechtmäßigkeit einer Verarbeitung betrifft.

21 Was die Beachtung von Art. 44 ff. DSGVO angeht, orientiert der Bayerische Landesbeauftragte für den Datenschutz seine Kontrollen vorrangig an den Dokumentationen, welche die Verantwortlichen zur Erfüllung der Rechenschaftspflicht erstellen. Verantwortliche können daher nicht erwarten, dass ihnen die Datenschutz-Aufsichtsbehörde die Erfüllung der Rechenschaftspflicht abnimmt; sie können insbesondere nicht erwarten, dass die Datenschutz-Aufsichtsbehörde die Zulässigkeit durchgeführter Drittstaatentransfers würdigt, wenn keine oder keine ausreichenden Dokumentationen vorgelegt werden können.

22 Bei Drittstaatentransfers im Zusammenhang mit Office-Anwendungen – ausgenommen sind Videokonferenz-Systeme – akzeptiert der Bayerische Landesbeauftragte für den Datenschutz unter den oben unter Rn. 4 ff. dargelegten Anforderungen bis auf weiteres grundsätzlich auch Dokumentationen zur Erfüllung der Rechenschaftspflicht, die auf eine Prüfung der tatsächlichen Wirksamkeit von Klauselwerken (siehe oben Rn. 10 f., 15) verzichten. Vorausgesetzt ist dabei,

- dass das vereinbarte Klauselwerk nach den Vorgaben unter Rn. 8 f., 14 auf den aktuellen Standarddatenschutzklauseln beruht und von diesen nicht abweicht, sowie
- dass der Verantwortliche nach den Vorgaben unter Rn. 11, 18 f. eine ausreichend sicher gestaltete Verschlüsselung und/oder Pseudonymisierung vorsieht und anwendet.

1 Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 203-3. Risikoanalyse auf der Basis von IT-Grundschutz, Internet: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html.

2 Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, ABl. L 199 vom 7. Juni 2021, S. 31 ff.

3 Vgl. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, Pressemitteilung vom 21. Juni 2021, Internet: https://www.datenschutzkonferenz-online.de/pressemitteilungen.html.

4 Europäischer Datenschutzausschuss, Recommendations 01/2020 vom 18. Juni 2021, Rn. 28 ff., Internet: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

5 Recommendations 01/2020, Rn. 50 ff.

6 Recommendations 01/2020, Rn. 54.

7 Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18, Rn. 177 ff.

8 Vgl. näher Recommendations 01/2020, Annex 3.

9 Zu diesem näher Europäischer Datenschutzausschuss/Europäischer Datenschutzbeauftragter, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection mit Annex vom 10. Juli 2019, Internet: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

10 Zu den Anforderungen näher a. a. O. (Endnote 9), Annex, S. 4 ff.