Der Bayerische Landesbeauftragte
für den Datenschutz

KI ohne Grenzen? Einsatz von Drittlandsprodukten in der bayerischen Verwaltung

Aktuelle Kurz-Information 60

Stichwörter: Datentransfers, internationale (KI) – Drittland-KI – Drittstaatenübermittlung (KI) – KI aus Drittland – Künstliche Intelligenz aus Drittland | **Stand:** 1. März 2025

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Die Datenschutz-Grundverordnung gilt nach Maßgabe des Niederlassungs- und des Marktortprinzips auch für Datenverarbeitungen bei Training und Produktiveinsatz von Drittland-KI.
- Die Vorgaben der Datenschutz-Grundverordnung können dabei sowohl Anbieter als auch Betreiber als Verantwortliche treffen.
- Bei Drittland-KI kommt den Vorgaben aus Art. 27, Art. 28 und Art. 44 ff. DSGVO besondere Bedeutung zu; (Cyber-)Sicherheitsmaßnahmen können zur Risikominimierung beitragen.

Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie der Digitalisierung. Ihr Potenzial lässt sich auch für eine Steigerung der Verwaltungseffizienz erschließen. Zunehmend leistungsfähige KI-Angebote unterschiedlicher Herkunft drängen auf den Markt. Bei bayerischen öffentlichen Stellen besteht mitunter eine gewisse Unsicherheit, inwiefern sich von diesem „Boom" profitieren lässt – gerade, wenn attraktive Tools von Anbietern stammen, die außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung beheimatet sind. Der vorliegende Beitrag befasst sich daher mit den Anforderungen aus den Bereichen Datenschutz (1.) und IT-Sicherheit (2.), denen bei Drittland-KI Rechnung getragen werden sollte. 1

1. Datenschutzrechtliche Anforderungen

Für Verarbeitungen personenbezogener Daten im Zusammenhang mit KI-Tools ist die Datenschutz-Grundverordnung zu beachten, wenn nach den allgemeinen Regeln ihr Anwendungsbereich eröffnet ist. 2

Verarbeitungen personenbezogener Daten kommen im Zusammenhang mit KI-Anwendungen vielfältig in Betracht, so beispielsweise 3

- im Rahmen des Trainings durch Erhebung und Nutzung von personenbezogenen Daten als **Trainingsdaten**,[1]
- bei der Nutzung in Form der **Erhebung, Aufzeichnung und Speicherung von Anmeldedaten und Eingabeaufforderungen** der Nutzenden (bei Großen Sprachmodellen [LLM] „Prompts") oder
- durch **Weiternutzung der Anmelde- und Eingabedaten zu eigenen Zwecken des Anbieters**, etwa zum Weitertraining der KI-Anwendung, zur Erstellung und Erkennung von Nutzerprofilen – nicht nur aufgrund der Nutzung der betreffenden KI-Anwendung an sich, sondern zum Beispiel auch aufgrund von Tastatureingabemustern – sowie zu Analyse- oder Werbezwecken.

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

4 Zur umfassenden Gewährleistung des in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz, Art. 8 Charta der Grundrechte der Europäischen Union verankerten Schutzes personenbezogener Daten findet die Datenschutz-Grundverordnung gemäß ihrem Art. 3 auf sämtliche Verarbeitungen personenbezogener Daten Anwendung, die in einem **Zusammenhang mit der Europäischen Union** stehen – **unabhängig von der Niederlassung des Verantwortlichen und dem Ort der Verarbeitung**.

5 Dabei gilt: **Verarbeitet eine KI-Anwendung personenbezogene Daten in der Europäischen Union** (sogenanntes Niederlassungsprinzip) **oder befinden sich die betroffenen Personen in der Europäischen Union** (sogenanntes Marktortprinzip), ist der **Anwendungsbereich** der Datenschutz-Grundverordnung eröffnet. Dann muss der datenschutzrechtlich Verantwortliche deren Anforderungen, **insbesondere** in Gestalt der **Verarbeitungsgrundsätze des Art. 5 Abs. 1 Datenschutz-Grundverordnung** (DSGVO) einhalten, **unter anderem**

- das zwingende Erfordernis einer **Rechtsgrundlage** für die Datenverarbeitung (**Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DSGVO**, bei Verarbeitungen besonderer Kategorien personenbezogener Daten in Verbindung mit **Art. 9 DSGVO**),
- den **Grundsatz der Zweckbindung** (**Art. 5 Abs. 1 Buchst. b DSGVO**, bei zweckändernden Weiterverarbeitungen **Art. 6 Abs. 4 DSGVO und Art. 6 Bayerisches Datenschutzgesetz** - BayDSG),
- die **Informationspflichten** (**Art. 5 Abs. 1 Buchst. a, Art. 12 ff. DSGVO**)[2] und
- die **Betroffenenrechte** (**Art. 15 ff. DSGVO**)[3].
- Hinzu treten bei **Nutzung von Produkten von Drittlandanbietern regelmäßig** die Vorgaben der **Art. 44 ff. DSGVO betreffend Datenverarbeitungen mit Drittlandbezug**.

6 Konkretisiert werden diese Vorgaben durch **Art. 24 Abs. 1 Satz 1, Art. 25, Art. 32 Abs. 1 DSGVO**, wonach unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen durch **geeignete technische und organisatorische Maßnahmen** sicherzustellen und nachzuweisen ist, dass die Verarbeitung im Einklang mit der Datenschutz-Grundverordnung erfolgt und ein dem Risiko angemessenes Schutzniveau gewährleistet wird.

7 Der datenschutzrechtlich Verantwortliche muss die Einhaltung der Anforderungen jederzeit nachweisen können (**Art. 5 Abs. 2 DSGVO „Rechenschaftspflicht“**).

8 **Datenschutzrechtlich Verantwortlicher** im Sinne des **Art. 4 Nr. 7 DSGVO** ist dabei die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dies ist je nach Verarbeitungsvorgang der Anbieter oder der Betreiber[4] einer KI-Anwendung: Geht es um **Verarbeitungen** personenbezogener Daten **im Zusammenhang mit der Entwicklung und dem Training** einer KI-Anwendung, ist in der Regel der **Anbieter** für deren Datenschutzkonformität verantwortlich. Für Datenverarbeitungen, die mit der **Nutzung** einer KI-Anwendung einhergehen, trifft die datenschutzrechtliche Verant-

wortlichkeit dagegen den **Betreiber** der jeweiligen KI-Anwendung, das heißt beispielsweise die jeweilige die **KI-Anwendung als Betriebsmittel einsetzende bayerische öffentliche Stelle**, gegebenenfalls in Zusammenarbeit mit dem Anbieter als Auftragsverarbeiter im Sinne des Art. 28 DSGVO.

a) Speziell: datenschutzrechtliche Anforderungen an Drittlandanbieter

Verarbeitet eine KI-Anwendung eines nicht in der Europäischen Union niedergelassenen Verantwortlichen personenbezogene Daten von **betroffenen Personen, die sich in der Europäischen Union befinden** (Art. 3 Abs. 2 Buchst. a DSGVO), ist der **Anwendungsbereich** der Datenschutz-Grundverordnung eröffnet und muss der Verantwortliche die oben genannten Anforderungen einhalten. 9

Der (Drittland-)Anbieter einer KI-Anwendung ist dabei regelmäßig für **Entwicklung und Training** datenschutzrechtlich **verantwortlich** im Sinne des Art. 4 Nr. 7 DSGVO. **Nicht in der Union niedergelassene Verantwortliche**, die im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen in der Union personenbezogene Daten von betroffenen Personen verarbeiten, die sich in der Union befinden (vgl. Art. 3 Abs. 2 Buchst. a DSGVO), müssen dabei nach Art. 27 Abs. 1 DSGVO **schriftlich einen Vertreter in der Union benennen**. Dies soll insbesondere die effektive Wahrnehmung und Durchsetzung der Betroffenenrechte ermöglichen und die Zusammenarbeit mit den europäischen Datenschutz-Aufsichtsbehörden erleichtern. 10

Stellt ein Anbieter **eine KI-Anwendung zur Nutzung durch einen Dritten als Verantwortlichen (Betreiber) bereit,** wird er je nach Einzelfallgestaltung gegebenenfalls als **Auftragsverarbeiter im Sinne der Art. 28, Art. 29, Art. 4 Nr. 8 DSGVO** tätig. Vorausgesetzt ist dabei, dass der Anbieter personenbezogene Daten (nur) im Auftrag und auf Weisung des Verantwortlichen verarbeitet.[5] In der Rolle des Auftragsverarbeiters muss der Anbieter hinreichende **Garantien** dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** eine **Verarbeitung im Einklang mit den Anforderungen der Datenschutz-Grundverordnung** sicherstellen und so der **Schutz der Rechte der betroffenen Personen gewährleistet** ist (vgl. Art. 28 Abs. 1 DSGVO). Der Inhalt des Auftragsverarbeitungsverhältnisses ist in einem **Vertrag oder anderen Rechtsinstrument** entsprechend den Vorgaben des **Art. 28 Abs. 3 DSGVO** zu regeln. **Bestimmt** ein Auftragsverarbeiter allerdings entgegen Art. 29, Art. 4 Nr. 8 DSGVO die **Zwecke und Mittel einer Verarbeitung** personenbezogener Daten, **ist er in Bezug auf diese Verarbeitung Verantwortlicher (Art. 28 Abs. 10 DSGVO)**. Dann treffen ihn auch die entsprechenden Pflichten. Das ist beispielsweise dann der Fall, wenn der Anbieter einer KI-Anwendung die Anmeldedaten und Eingabeaufforderungen des Betreibers als Verantwortlichen ohne dessen entsprechende Weisung erhebt, aufzeichnet und speichert oder wenn er diese Daten zu eigenen Zwecken wie dem Weitertraining der KI-Anwendung nutzt. 11

b) Speziell: datenschutzrechtliche Anforderungen an bayerische öffentliche Stellen als Betreiber

12 Nutzt eine bayerische öffentliche Stelle als Betreiber eine KI-Anwendung als Betriebsmittel zur Aufgabenerfüllung, ist die öffentliche Stelle insoweit datenschutzrechtlich Verantwortlicher, Art. 4 Nr. 7 Halbsatz 2 DSGVO in Verbindung mit **Art. 3 Abs. 2, Art. 1 BayDSG**. Sie muss die datenschutzkonforme Nutzung sicherstellen und nachweisen (Art. 5 Abs. 2 DSGVO). Der Verantwortliche muss dabei in Hinblick auf Art. 24 Abs. 1 und 2 DSGVO auch nachweisen können, dass er einer **Pflicht zur „angemessenen Bewertung“**[6] der Datenschutzkonformität der als Betriebsmittel eingesetzten KI-Anwendung nachgekommen ist, und dass er – soweit erforderlich – eine Umsetzung sogenannter **„mitigierender Maßnahmen“** geprüft hat.[7]

13 Wird die KI-Anwendung dabei ausschließlich **in eigener Verantwortlichkeit** (On-Premises, On-Prem) **und in einem abgeschotteten System** betrieben, besteht eine **Alleinverantwortlichkeit** der öffentlichen Stelle bezüglich sämtlicher Datenschutzaspekte.

14 Greift eine öffentliche Stelle für eine Verarbeitung personenbezogener Daten auf eine externe KI-Anwendung zurück, wird deren (Drittland-)Anbieter je nach Einzelfallgestaltung gegebenenfalls als **Auftragsverarbeiter im Sinne der Art. 28, Art. 29, Art. 4 Nr. 8 DSGVO im Auftrag und auf Weisung für die öffentliche Stelle** als Verantwortlichen tätig. Die öffentliche Stelle darf dabei ausweislich **Art. 28 Abs. 1 DSGVO** nur mit solchen Auftragsverarbeitern arbeiten, die **hinreichend Garantien** dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im **Einklang mit den Anforderungen der Datenschutz-Grundverordnung** erfolgt und den **Schutz der Rechte der betroffenen Personen** gewährleistet. Dazu gehören auch die Einhaltung der gesetzlichen Vorgaben zu Drittstaatentransfers (Art. 44 ff. DSGVO, vgl. Rn. 15 f.) sowie der Ausschluss von Verarbeitungen zu eigenen Zwecken des Anbieters. Den Verantwortlichen trifft insoweit eine **fortlaufende Prüf- und Überwachungspflicht**. Das Auftragsverarbeitungsverhältnis ist durch einen **Vertrag oder ein anderes Rechtsinstrument** entsprechend den Vorgaben des **Art. 28 Abs. 3 DSGVO** zu regeln.

15 Nutzt eine bayerische öffentliche Stelle eine KI-Anwendung eines **Drittlandanbieters**, ist ein besonderer Fokus auf die Voraussetzungen der Art. 44 ff. DSGVO zu legen, da es im Zusammenhang mit der Nutzung der KI-Anwendung regelmäßig zu **Datenübermittlungen** der nutzenden öffentlichen Stelle als Datenexporteur an den Anbieter als Datenimporteur **in Länder außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung**, das heißt der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums (sogenannte Drittländer), kommt. **Typischerweise** finden Drittlandübermittlungen bei der Nutzung einer (fremdentwickelten) KI-Anwendung eines Drittlandanbieters als **Cloud**-Lösung statt, wenn der Server der Cloud sich ebenfalls in einem Drittland befindet oder unabhängig vom Serverstandort zumindest Meta- und Telemetriedaten in ein Drittland übermittelt werden; in diesem Fall stellt sich zudem die Frage der Datensouveränität.[8] Denkbar ist auch eine Drittlandübermittlung aufgrund der **(gesetzlich angeordneten) Einräumung von Zugriffsrechten** auf eine KI-Anwendung (und die darin enthaltenen personenbezogenen Daten) für **drittstaatliche (Sicherheits-)Behörden** oder verbundene Unternehmen.[9]

Liegt ein solcher Drittstaatentransfer vor, spezifizieren **Art. 44 ff. DSGVO** die zusätzlichen Anforderungen an die Rechtmäßigkeit der Übermittlung personenbezogener Daten an Drittländer.[10] 16

- Hierbei ist zunächst zu prüfen, ob ein **gültiger Angemessenheitsbeschluss der Europäischen Kommission** für das Drittland im Sinne von **Art. 45 Abs. 1 und 3 DSGVO** vorliegt. 17
- Ist dies nicht der Fall beziehungsweise ist ein Angemessenheitsbeschluss auf den betreffenden Sachverhalt nicht anwendbar, kommt eine **Datenübermittlung vorbehaltlich geeigneter Garantien (vgl. EG 108 DSGVO) sowie durchsetzbarer Rechte und wirksamer Rechtsbehelfe für die betroffenen Personen gemäß Art. 46 Abs. 1 DSGVO** in Betracht, vorausgesetzt diese Garantien gewährleisten ein Schutzniveau für die übermittelten personenbezogenen Daten, das dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist. Ist dem Anbieter als Datenimporteur nach der Rechtslage im Drittland die **Einhaltung seiner vertraglichen Verpflichtungen nicht möglich, beispielsweise aufgrund gesetzlicher Zugriffsbefugnisse für drittstaatliche (Sicherheits-)Behörden** auf die verarbeiteten personenbezogenen Daten, muss der Verantwortliche als Datenexporteur auf der Grundlage einer umfassenden **Prüfung der Datenschutzsituation im Drittland zusätzliche Maßnahmen** ergreifen, die geeignet sind, die Einhaltung des Schutzniveaus zu gewährleisten. 18
- Kann die Übermittlung weder auf einen Angemessenheitsbeschluss nach Art. 45 Abs. 1 DSGVO noch auf geeignete Garantien nach Art. 46 Abs. 1 DSGVO gestützt werden, sieht **Art. 49 DSGVO als Auffangtatbestand** Ausnahmen für bestimmte Fälle von Drittlandübermittlungen vor. 19

Mit Blick auf die **Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO** ist es bayerischen öffentlichen Stellen daher zu empfehlen, grundsätzlich nicht mit Drittlandanbietern von KI-Anwendungen zusammenzuarbeiten, die intransparent im Hinblick auf die von ihnen (im Auftrag) vorgenommene Verarbeitung personenbezogener Daten agieren. 20

Unter Beachtung der **Art. 24 Abs. 1 Satz 1, Art. 25, Art. 32 Abs. 1 DSGVO**[11] kann der On-Prem-Betrieb von KI-Systemen eine Maßnahme zur Risikominimierung und Gewährleistung des Datenschutzes darstellen. Durch die Kontrolle über die physische und logische Infrastruktur, auf der die KI-Anwendung betrieben wird, können bayerische öffentliche Stellen sicherstellen, dass die Datenverarbeitung im Einklang mit den datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung steht. So kann die in Art. 25 DSGVO geforderte Datensicherheit durch Technikgestaltung und datenschutzfreundliche Voreinstellungen leichter umgesetzt werden. Eine aktive Steuerung der Sicherheitsmaßnahmen kommt der Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten zugute; die Abhängigkeit von externen Drittanbietern wird reduziert. Der On-Prem-Betrieb entbindet bayerische öffentliche Stellen jedoch nicht von ihrer Verantwortung, erforderliche Maßnahmen nach Art. 32 Abs. 1 DSGVO zu treffen. Um ein angemessenes Schutzniveau zu erreichen, muss stets in einer umfassenden Risikoanalyse geklärt werden, welche Risiken bestehen und wie ihnen zu begegnen ist. 21

22 Sind die **datenschutzrechtlichen Vorgaben nicht vollumfänglich erfüllt**, **verstößt** die betreffende Verarbeitung personenbezogener Daten mittels einer KI-Anwendung **gegen die Datenschutz-Grundverordnung**. Dies sollten öffentliche Stellen bei der Auswahl, der Beschaffung[12] und dem Einsatz entsprechender KI-Anwendungen, einschließlich der Etablierung technisch-organisatorischer Sicherungsmaßnahmen, beachten. Beschäftigte der öffentlichen Stellen sollten hierfür sensibilisiert werden.

2. KI-Verordnung und Cybersicherheit

23 Über diese datenschutzrechtlichen Problemstellungen hinaus sind unter anderem Anforderungen aus der KI-Verordnung[13] (speziell hinsichtlich Transparenz) sowie betreffend die Cybersicherheit zu beachten. Letztere steht insbesondere bei potenziellen Zugriffsmöglichkeiten drittstaatlicher (Sicherheits-)Behörden, bei schwachen Sicherheitsvorkehrungen und bei einer möglichen Manipulierbarkeit von KI-Anwendungen (für kriminelle Zwecke) in Frage.

24 Eine kürzlich bekannt gewordene Datenpanne bei einer Drittland-KI verdeutlicht die Risiken, die mit unzureichenden Sicherheitsmaßnahmen bei KI-Anwendungen verbunden sind: Aufgrund einer Fehlkonfiguration war eine Datenbank mit über einer Million sensibler Datensätze, darunter Chatverläufe und Systemprotokolle, ungeschützt und öffentlich im Internet erreichbar. Die Sicherheitslücke erlaubte nicht nur den Zugriff auf vertrauliche Informationen, sondern eröffnete auch die Möglichkeit zur Manipulation der Datenbank. Obwohl das Unternehmen nach der Entdeckung schnell reagierte und die Datenbank sicherte, bleibt nicht nur unklar, wie lange die Daten vorher exponiert waren, sondern auch, ob unbefugte Dritte darauf zugegriffen haben. Dieser Vorfall unterstreicht die Notwendigkeit wirksamer Sicherheitsanforderungen für KI-Anwendungen, insbesondere wenn diese aus Ländern stammen, in denen Datenschutz- und Sicherheitsstandards möglicherweise nicht den europäischen Anforderungen entsprechen.

1 Bayerischer Landesbeauftragter für den Datenschutz, Fotos veröffentlichen = KI trainieren?, Aktuelle Kurz-Information 55, Stand 4/2024, Internet: https://www.datenschutz-bayern.de/infothek.

2 Bayerischer Landesbeauftragter für den Datenschutz, Informationspflichten des Verantwortlichen, Orientierungshilfe, Stand 11/2018, Internet: https://www.datenschutz-bayern.de/infothek.

3 Bayerischer Landesbeauftragter für den Datenschutz, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 12/2019, und Das Recht auf Löschung nach der Datenschutz-Grundverordnung, Orientierungshilfe, Stand 6/2022, Internet: https://www.datenschutz-bayern.de/infothek.

4 Begrifflichkeiten in Anlehnung an Art. 3 Nr. 3 und 4 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. EU L 2024/1689 vom 12. Juli 2024, S. 1 ff.

5 Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Stand 4/2019, Internet: https://www.datenschutz-bayern.de/infothek.

6 Europäischer Datenschutzausschuss, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, Stand 12/2024, Rn. 122, Internet: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de. Die Aufsichtsbehörden sollten dabei unter anderem berücksichtigen, ob der Verantwortliche beispielsweise die für das der Anwendung zugrundeliegende KI-Modell verwendete Datenquelle und einen

möglichen (gegebenenfalls aufsichtsbehördlich oder gerichtlich festgestellten) Verstoß des KI-Modells gegen die Datenschutz-Grundverordnung bewertet hat. Der Grad der Bewertung des Verantwortlichen und der von den Aufsichtsbehörden erwartete Detaillierungsgrad können dabei in Abhängigkeit von verschiedenen Faktoren variieren, einschließlich der Art und des Ausmaßes der Risiken, die durch die Verarbeitung im KI-Modell während seines Einsatzes in Bezug auf die betroffenen Personen, deren Daten zur Entwicklung des Modells verwendet wurden, entstehen, Rn. 130.

7 Hierzu Europäischer Datenschutzausschuss, Opinion 28/2024 (Endnote 6), Rn. 132, 134.

8 Zu den mit Cloud-Services verbundenen Problemstellungen vgl. Bayerischer Landesbeauftragter für den Datenschutz, Datenschutz als Kriterium im Vergabeverfahren, Orientierungshilfe, Stand 2/2024, Internet: https://www.datenschutz-bayern.de/infothek.

9 Juarez, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, Stand 5/2023, Art. 44 DSGVO Rn. 15; Schröder, in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 44 DSGVO Rn. 16; Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers, Orientierungshilfe, Stand 5/2023, Rn. 28 ff., Internet: https://www.datenschutz-bayern.de/infothek.

10 Zum Ganzen ausführlich Bayerischer Landesbeauftragter für den Datenschutz, Internationale Datentransfers (Endnote 9) und Erste Hilfe zum Angemessenheitsbeschluss für das EU-U-S. Data Privacy Framework, Aktuelle Kurz-Information 51, Stand 12/2023, Internet: https://www.datenschutz-bayern.de/infothek.

11 Bayerischer Landesbeauftragter für den Datenschutz, Die Datenschutz-Grundverordnung – Anforderungen an Technik und Sicherheit der Verarbeitung, Stand 11/2017, Internet: https://www.datenschutz-bayern.de/infothek.

12 Zur Berücksichtigung von Datenschutz als Kriterium im Vergabeverfahren Endnote 8.

13 Endnote 4.