Der Bayerische Landesbeauftragte
für den Datenschutz

Internationaler Datenverkehr unter der Datenschutz-Grundverordnung

Arbeitspapier

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

Inhalt

Version 2.0 | Stand: 1. August 2020

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt. Es kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018" abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Die Datenschutz-Grundverordnung (DSGVO) verfolgt das Ziel, ein **einheitlich hohes Schutzniveau** für personenbezogene Daten in den Mitgliedstaaten der Europäischen Union (EU) sowie – nach Integration der Datenschutz-Grundverordnung in das Abkommen über den Europäischen Wirtschaftsraum (EWR)[1] – in Island, Liechtenstein und Norwegen als Mitgliedstaaten der Europäischen Freihandelszone (EFTA) zu gewährleisten. Dieses hohe Schutzniveau soll durch die Übermittlung personenbezogener Daten aus Ländern der EU und des EWR an Verantwortliche, Auftragsverarbeiter oder andere Empfänger in Drittländern (also in Ländern außerhalb der EU und des EWR) oder an internationale Organisationen **nicht untergraben** werden. 1

Beispiel: Durch Betriebssysteme können personenbezogene Daten in Drittländer übermittelt werden, etwa im Rahmen von Cloud-Speicher-Angeboten. Bayerische öffentliche Stellen (Schulen, Universitäten, Kommunen usw.) haben sich daher vor dem Einsatz eines entsprechenden Produkts mit dieser Problematik zu befassen. In diesem Zusammenhang kann auch das IT-Grundschutz-Kompendium des Bundesamtes für Sicherheit in der Informationstechnik[2] hilfreich sein.

Das vorliegende Arbeitspapier stellt die Voraussetzungen für eine Übermittlung personenbezogener Daten an ein Drittland – die in Art. 44 ff. DSGVO gewählte Formulierung erfasst auch Datenübermittlungen an beliebige Empfänger in dem Drittland – oder an eine internationale Organisation dar. Dabei geht es zunächst auf die Struktur der Zulässigkeitsprüfung (Rn. 4 ff.) und anschließend auf die wesentlichen Fallgruppen der Art. 44 ff. DSGVO (Rn. 11 ff.) ein. 2

In Bezug auf Verwaltungsbereiche, die in den Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz[3] fallen, gelten Art. 44 ff. DSGVO nicht. Der bayerische Gesetzgeber hat Kapitel V DSGVO, dem die Vorschriften angehören, nicht in seine Anwendbarerklärung eingeschlossen (vgl. Art. 2 Satz 1, Art. 28 Abs. 2 Bayerisches Datenschutzgesetz). Allerdings bestehen fachgesetzliche Vorgaben, beispielsweise in Art. 58 Polizeiaufgabengesetz sowie in §§ 77d ff. Gesetz über die internationale Rechtshilfe in Strafsachen. 3

1. Zweistufige Zulässigkeitsprüfung

Falls eine bayerische öffentliche Stelle personenbezogene Daten an Empfänger in Drittländern oder an internationale Organisationen übermitteln will, muss sie – wie auch schon nach bisheriger Rechtslage – eine **zweistufige Zulässigkeitsprüfung** vornehmen: 4

a) Erste Prüfungsstufe: allgemeine datenschutzrechtliche Übermittlungsvoraussetzungen

5 Die bayerische öffentliche Stelle muss – wie bei jeder Datenverarbeitung – die allgemeinen Rechtmäßigkeitsvoraussetzungen der Art. 5 ff. DSGVO einhalten. So müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Insbesondere muss ein Erlaubnistatbestand für die jeweilige Verarbeitung vorliegen. Außerdem sind auch die Grundsätze der „Zweckbindung", „Datenminimierung", „Richtigkeit", „Speicherbegrenzung" sowie der „Integrität und Vertraulichkeit" zu beachten (vgl. Art. 5 Abs. 1 DSGVO).[4] Der Verantwortliche unterliegt insofern einer „Rechenschaftspflicht" (vgl. Art. 5 Abs. 2 DSGVO).

6 Häufig wird eine Auftragsverarbeitung vorliegen.[5] Im Falle einer Auftragsverarbeitung sind insbesondere die Vorgaben des Art. 28 DSGVO zu beachten.

Beispiel: Eine bayerische öffentliche Stelle will einen Cloud-Anbieter nutzen, wobei die Datenverarbeitung zumindest teilweise außerhalb der EU und des EWR stattfinden soll.

b) Zweite Prüfungsstufe: spezifische Anforderungen für die Übermittlung an Drittländer oder internationale Organisationen

7 Zusätzlich muss die übermittelnde bayerische öffentliche Stelle die Vorgaben der Art. 44 ff. DSGVO einhalten. Die Vorschriften der Art. 44 ff. DSGVO umfassen drei wesentliche Fallgruppen:

- Datenübermittlungen auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO, Rn. 11 ff.);
- Datenübermittlungen vorbehaltlich geeigneter Garantien (Art. 46 DSGVO, Rn. 21 ff.) und
- Datenübermittlungen in bestimmten Ausnahmefällen (Art. 49 DSGVO, Rn. 33 ff.).

8 Der Begriff der Datenübermittlung erfasst hier grundsätzlich **sämtliche Formen der Drittlandgrenzüberschreitung von Daten**. Dies gilt beispielsweise für das Weitergeben von Daten an einen Empfänger im Drittland, aber auch für die sonstige Bereitstellung, Zugänglichkeit im oder Abrufbarkeit aus dem Drittland, weiterhin für das Speichern auf Servern, die in einem Drittland gelegen sind.

9 Auch die Weitergabe von Daten an einen Auftragsverarbeiter in einem Drittland ist eine Datenübermittlung im Sinne der Art. 44 ff. DSGVO (vgl. Art. 4 Nr. 9 DSGVO). Neben Art. 28 f. DSGVO (siehe erste Prüfungsstufe, Rn. 5 f.) sind daher bei einer Auftragsverarbeitung in einem Drittland auch die Art. 44 ff. DSGVO zu beachten.

10 Für Sozialdaten hat Deutschland im Zehnten Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) von der in Art. 49 Abs. 5 DSGVO eingeräumten Abweichungsmöglichkeit Gebrauch gemacht und die Übermittlung von Sozialdaten beschränkt

(§ 77 Abs. 3 SGB X, für Auftragsverarbeitung § 80 Abs. 2 SGB X). Dadurch will der Gesetzgeber gewährleisten, dass Sozialdaten nicht in datenschutzrechtlich unsichere Drittstaaten übermittelt werden.[6]

2. Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO)

Nach Art. 45 Abs. 1 DSGVO kann die Europäische Kommission beschließen, dass ein bestimmtes Drittland oder eine bestimmte internationale Organisation ein „angemessenes Schutzniveau" bietet. Vorgaben zum Prüfungsmaßstab der Europäischen Kommission enthält Art. 45 Abs. 2 DSGVO.[7] Der Europäische Datenschutzausschuss (bisher: Datenschutzgruppe nach Artikel 29) hat dazu das Arbeitspapier „Referenzgrundlage für Angemessenheit"[8] veröffentlicht. 11

Ein bekanntes Beispiel für einen „Angemessenheitsbeschluss" betrifft das Verhältnis der EU zu den Vereinigten Staaten von Amerika (sog. EU-US-Datenschutzschild).[9] Diesen Beschluss hat der Europäische Gerichtshof allerdings für ungültig erklärt.[10] 12

Hintergrund: Dem EU-US-Datenschutzschild liegt der Gedanke zugrunde, dass sich US-amerikanische Organisationen als Datenempfänger gegenüber dem US-Handelsministerium per freiwilliger Selbstzertifizierung verpflichten, die niedergelegten datenschutzrechtlichen Grundsätze einzuhalten. Die Einhaltung dieser freiwilligen Selbstverpflichtungen soll durch eine US-amerikanische Aufsichtsinstanz überwacht werden. Insoweit sollte der EU-US-Datenschutzschild ein angemessenes Schutzniveau für personenbezogene Daten sicherstellen, die in seinem Rahmen aus der EU an Organisationen in den Vereinigten Staaten übermittelt werden. 13

Der Europäische Gerichtshof hat erkannt, dass der EU-US-Datenschutzschild ebenso wie der im Jahr 2015[11] für ungültig erklärte „Safe-Harbor-Mechanismus"[12] den US-amerikanischen Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen Vorrang vor Datenschutzaspekten einräumt. US-amerikanische Behörden könnten auf Basis nachrichtendienstlicher Überwachungsprogramme durch Zugriffs- und Verwendungsmöglichkeiten hinsichtlich der übermittelten personenbezogenen Daten in die grundrechtlich geschützte Sphäre betroffener Personen eingreifen. 14

Der Europäische Gerichtshof ist bei seiner Prüfung zu dem Ergebnis gekommen, dass das US-amerikanische Recht kein im Sinne von Art. 45 DSGVO angemessenes Schutzniveau gewährleisten könne, da es im Hinblick auf Grundrechtseingriffe nicht die erforderlichen Einschränkungen und Garantien vorsehe und auch keinen effektiven gerichtlichen Rechtsschutz vor solchen Eingriffen gewährleiste. 15

Regelungen von Grundrechtseingriffen durch US-amerikanische Behörden müssten Anforderungen erfüllen, die den in Art. 52 Abs. 1 Satz 2 Charta der Grundrechte der Europäischen Union niedergelegten Verhältnismäßigkeitsmaßstäben der Sache nach gleichwertig wären. Die US-amerikanischen Überwachungsprogramme ermöglichten jedoch Sammelerhebungen ohne hinreichend klare und präzise Eingrenzung des Umfangs und ohne ausreichende 16

Möglichkeit einer gerichtlichen Kontrolle. Auch der im EU-US-Datenschutzschild vorgesehene Ombudsmechanismus konnte an dieser Einschätzung nichts ändern, da zum einen die Unabhängigkeit der Ombudsperson aus Sicht des Europäischen Gerichtshofs zweifelhaft ist und zum anderen diese nicht ermächtigt ist, verbindliche Entscheidungen gegenüber US-amerikanischen Nachrichtendiensten zu erlassen.

17 Im Ergebnis können Datenübermittlungen in die USA derzeit mangels gültigen Angemessenheitsbeschlusses nicht auf Grundlage von Art. 45 DSGVO vorgenommen werden. Insoweit können die in Art. 49 DSGVO geregelten Ausnahmen für bestimmte Fälle (siehe Rn. 33 ff) bedeutsam sein.

18 Gültige Angemessenheitsbeschlüsse bestehen dagegen in Bezug auf Andorra, Argentinien, Kanada, Israel, Japan, Neuseeland, die Schweiz und Uruguay, die Färöer-Inseln sowie die Inseln Guernsey, Jersey und Man. Die Datenschutz-Grundverordnung sieht die grundsätzliche **Fortgeltung der bereits erlassenen Angemessenheitsbeschlüsse** vor (Art. 45 Abs. 9 DSGVO).

19 Angemessenheitsbeschlüsse beziehen sich nicht zwangsläufig auf alle Verarbeitungssituationen im Empfängerland der Daten. Der Bereich der Strafverfolgung ist regelmäßig ausgenommen. Im Fall Kanada gilt die Angemessenheitsentscheidung beispielsweise nur für solche Datenverarbeitungen, die dem Personal Information Protection and Electronic Documents Act[13] unterfallen.[14]

20 Vor einer Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission ist daher zu prüfen, ob sie von dessen Anwendungsbereich umfasst ist. Fällt diese Prüfung positiv aus, können Daten übermittelt werden. Weitere Anforderungen – wie etwa das Vorliegen geeigneter Garantien nach Art. 46 DSGVO – sind dann nicht mehr zu prüfen.

3. Vorliegen geeigneter Garantien (Art. 46 DSGVO)

21 Art. 46 Abs. 1 DSGVO erlaubt die Datenübermittlung an ein Drittland oder eine internationale Organisation, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (siehe Rn. 30). Für bayerische öffentliche Stellen sind folgende mögliche Garantien hervorzuheben:

a) Rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen (Art. 46 Abs. 2 Buchst. a DSGVO)

22 Eine durch die Datenschutz-Grundverordnung neu eingeführte Garantie zur Rechtfertigung von Datenübermittlungen bei fehlendem Angemessenheitsbeschluss stellen gemäß Art. 46 Abs. 2 Buchst. a DSGVO rechtlich bindende und durchsetzbare Dokumente zwischen den Behörden oder öffentlichen Stellen dar. Rechtsverbindlichkeit und Durchsetzbarkeit liegen dabei nur dann vor, wenn die betroffenen Personen die Möglichkeit haben, die ihnen in dem

Dokument gewährleisteten Rechte durchzusetzen. Ihnen muss das Dokument somit **effektive verwaltungsrechtliche und gerichtliche Rechtsbehelfe sowie das Recht auf Schadensersatz** einräumen. Bei „verwaltungsrechtlichen Rechtsbehelfen" handelt es sich auch um das Recht auf Anrufung einer Datenschutz-Aufsichtsbehörde.

Ausdrücklich nicht von der Vorschrift umfasst sind Verwaltungsvereinbarungen ohne rechtsverbindlichen Charakter. Für diese kann allerdings Art. 46 Abs. 3 Buchst. b DSGVO greifen. Sie bedürfen dann – anders als die rechtlich bindenden und durchsetzbaren Dokumente im Sinn von Art. 46 Abs. 2 Buchst. a DSGVO – vorab einer Genehmigung durch die zuständige Datenschutz-Aufsichtsbehörde. 23

b) „Standarddatenschutzklauseln" (Art. 46 Abs. 2 Buchst. c DSGVO)

Wurde dem betreffenden Drittland oder der betreffenden internationalen Organisation von der Europäischen Kommission kein angemessenes Datenschutzniveau attestiert, kann grundsätzlich auf die ebenfalls von der Europäischen Kommission vorformulierten Standardvertragsklauseln zurückgegriffen werden, um ausreichende Garantien für die Übermittlung personenbezogener Daten zu schaffen. Die Datenschutz-Grundverordnung verwendet lediglich den neuen Begriff „Standarddatenschutzklauseln". 24

Gegenwärtig existieren drei Klauselwerke, die gemäß Art. 46 Abs. 5 Satz 2 DSGVO vorerst fortgelten: 25

- Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß Entscheidung der Kommission 2001/497/EG;[15]
- sog. alternative Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß Entscheidung der Kommission 2004/915/EG;[16]
- Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern 2010/87/EU.[17]

Die Europäische Kommission wurde von mehreren Mitgliedstaaten (darunter Deutschland) nachdrücklich gebeten, diese Standardvertragsklauseln zeitnah mit Blick auf die Anforderungen des Art. 28 f. DSGVO (Auftragsverarbeitung) zu überarbeiten. 26

Der Europäische Gerichtshof hat die Gültigkeit der Standardvertragsklauseln gemäß Beschluss der Kommission 2010/87/EU – am Maßstab der Charta der Grundrechte der Europäischen Union gemessen – mit Urteil vom 16. Juli 2020 zwar bestätigt.[18] 27

Nach Auffassung des Europäischen Gerichtshofs müssen die Rechte der von der Datenübermittlung in ein Drittland betroffenen Person jedoch ein Schutzniveau genießen, das dem durch die Datenschutz-Grundverordnung garantierten Niveau gleichwertig ist. Insoweit maßgeblich seien die zwischen dem in der EU ansässigen Datenexporteur und dem im Drittland ansässigen Datenempfänger getroffenen vertraglichen Vereinbarungen und die maßgeblichen Aspekte der Rechtsordnung des Drittlandes, was einen etwaigen Zugriff der dortigen Behörden auf die übermittelten Daten betrifft. 28

29 Standarddatenschutzklauseln binden den Datenexporteur und den Datenimporteur, sofern sie einen Vertrag unter Bezugnahme auf diese Klauseln geschlossen haben. Anders als ein Angemessenheitsbeschluss im Sinne von Art. 45 Abs. 3 DSGVO treffen Standarddatenschutzklauseln aber keine Aussagen über das Datenschutzniveau eines bestimmten Staates. So kann es durchaus zu Situationen kommen, in denen die Standarddatenschutzklauseln kein effektives Datenschutzniveau gewährleisten können, etwa wenn das Recht des Drittlandes den dortigen Behörden Eingriffe in die Rechte der betroffenen Personen erlaubt.

30 Derartige Situationen führen aber nicht zwangsläufig zur Unwirksamkeit der Standarddatenschutzklauseln. Es liegt dann vielmehr im Verantwortungsbereich des in der EU ansässigen Verantwortlichen oder seines dort ansässigen Auftragsverarbeiters, zusätzliche Maßnahmen zu ergreifen, um die Einhaltung des unionsrechtlich geforderten Schutzniveaus im Drittland zu gewährleisten. Hierzu muss er in jedem Einzelfall – gegebenenfalls in Zusammenarbeit mit dem Empfänger der Übermittlung – prüfen, ob das Recht des Bestimmungsdrittlands ein angemessenes Schutzniveau gewährleistet, und erforderlichenfalls mehr Garantien als die durch die Standarddatenschutzklauseln gebotenen gewähren. Ist die Einhaltung der Standarddatenschutzklauseln unmöglich, etwa weil das Recht des Drittlands ihre tatsächliche Wirkung vereitelt, oder wird gegen ihre Einhaltung verstoßen, so ist die Datenübermittlung auszusetzen oder zu beenden.

31 Kommen Datenschutz-Aufsichtsbehörden zu dem Ergebnis, dass ein angemessener Schutz der auf Grundlage der Standarddatenschutzklauseln übermittelten Daten nicht gewährleistet wird oder werden kann, so haben sie die Aussetzung der Übermittlung personenbezogener Daten auf Grundlage der Standarddatenschutzklauseln in das Drittland anzuordnen (Art. 58 Abs. 2 Buchst. j DSGVO) oder zu verbieten (Art. 58 Abs. 2 Buchst. f DSGVO).

c) Zertifizierung (Art. 46 Abs. 2 Buchst. f DSGVO)

32 Zertifizierungen sieht die Datenschutz-Grundverordnung als neues Instrument vor. An einem Zertifizierungsmechanismus teilnehmende Verantwortliche und Auftragsverarbeiter in Drittländern oder internationalen Organisationen müssen rechtsverbindliche und durchsetzbare Verpflichtungen zur Anwendung der geeigneten Garantien, auch hinsichtlich der Rechte der betroffenen Personen, eingehen (Art. 46 Abs. 2 Buchst. f in Verbindung mit Art. 42 Abs. 2 DSGVO). Die zuständige Datenschutz-Aufsichtsbehörde muss die Zertifizierungskriterien genehmigen; bei Bedarf muss sie das Kohärenzverfahren gemäß Art. 63 DSGVO durchführen (Art. 42 Abs. 5 DSGVO). Die Zertifizierungskriterien sollen geeignete Garantien zum Schutz der personenbezogenen Daten gewährleisten.[19]

4. Ausnahmen für bestimmte Fälle (Art. 49 DSGVO)

33 Eine Datenübermittlung an ein Drittland oder an eine internationale Organisation kann nach Art. 49 DSGVO in einer Reihe besonderer, abschließend genannter Fälle auch zulässig sein, wenn weder ein Angemessenheitsbeschluss der Europäischen Kommission noch geeignete

Garantien vorliegen. Wegen des Ausnahmecharakters ist diese Vorschrift eng auszulegen. Für bayerische öffentliche Stellen ist insbesondere auf Folgendes hinzuweisen:[20]

a) Einwilligung (Art. 49 Abs. 1 UAbs. 1 Buchst. a DSGVO)

Als Ausnahme ist die Einwilligung für **Behörden** in Ausübung ihrer **hoheitlichen Befugnisse** gemäß Art. 49 Abs. 3 DSGVO **ausdrücklich ausgeschlossen**. 34

Sofern dieser Ausnahmetatbestand für bayerische öffentliche Stellen demnach überhaupt noch in Betracht kommt, ist Folgendes zu beachten: 35

Der Begriff der Einwilligung ist in Art. 4 Nr. 11 DSGVO gesetzlich definiert. Danach ist eine Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung". Die betroffene Person ist dabei auch über das jederzeitige Widerrufsrecht zu informieren (Art. 7 Abs. 3 DSGVO). 36

Zusätzlich zu diesen für alle Einwilligungen geltenden Voraussetzungen[21] verlangt Art. 49 Abs. 1 UAbs. 1 Buchst. a DSGVO noch zweierlei: 37

- Die betroffene Person muss über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet worden sein, also insbesondere darüber, dass kein angemessenes Datenschutzniveau gegeben ist und Betroffenenrechte gegebenenfalls nicht durchgesetzt werden können.
- Außerdem muss die betroffene Person ihre Einwilligung ausdrücklich abgegeben haben.

Für die wiederholte, massenhafte oder routinemäßige Übermittlung personenbezogener Daten kommt dieser Ausnahmetatbestand somit regelmäßig nicht in Betracht.[22] Der Europäische Datenschutzausschuss sieht die **Anonymisierung** als vorzugswürdig an (konkret zum Forschungsbereich).[23] 38

In Anbetracht des ohnehin eingeschränkten Anwendungsbereichs, der aufgezeigten hohen Wirksamkeitshürden und der jederzeitigen Widerrufbarkeit erscheint dieser Ausnahmetatbestand für bayerische öffentliche Stellen im Ergebnis allenfalls in eng begrenzten Einzelfällen als Lösung geeignet. 39

b) Wichtige Gründe des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 Buchst. d DSGVO)

Die Übermittlung kann aus **wichtigen Gründen des öffentlichen Interesses notwendig** sein. Wie aus Erwägungsgrund (ErwGr) 112 DSGVO hervorgeht, meinte der Verordnungsgeber hiermit insbesondere Datentransfers im Rahmen der internationalen behördlichen Zusammenarbeit, etwa zwischen Wettbewerbs-, Steuer- oder Zollbehörden. Bei dieser Ausnahme ist Art. 49 Abs. 4 DSGVO zu beachten, wonach das öffentliche Interesse gesetzlich anerkannt sein muss. 40

c) Schutz lebenswichtiger Interessen (Art. 49 Abs. 1 UAbs. 1 Buchst. f DSGVO)

41 Die Übermittlung ist zulässig, wenn sie zum **Schutz lebenswichtiger Interessen** der betroffenen Person oder anderer Personen erforderlich ist, sofern die betroffene Person aus physischen oder rechtlichen Gründen zur Erteilung der Einwilligung außerstande ist. Zu den lebenswichtigen Interessen zählen insbesondere die körperliche Unversehrtheit und das Leben (ErwGr 112 Satz 2 DSGVO).

42 In der Praxis ist hier an Situationen zu denken, in denen sich die betroffene oder eine andere Person in einem lebensbedrohlichen Zustand befindet und es zur Rettung erforderlich ist, Daten der betroffenen Person etwa an Ärztinnen und Ärzte in einem Drittland zu übermitteln. Ist die betroffene Person bewusstlos und deshalb außerstande, eine Einwilligung abzugeben, kann von Art. 49 Abs. 1 UAbs. 1 Buchst. f DSGVO Gebrauch gemacht werden.

d) Übermittlung aus einem Register (Art. 49 Abs. 1 UAbs. 1 Buchst. g DSGVO)

43 Eine Übermittlung aus einem Register, das nach Unions- oder mitgliedstaatlichem Recht zur **Information der Öffentlichkeit bestimmt** ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, ist ein weiterer möglicher Ausnahmefall. Dies setzt aber unter anderem voraus, dass die im Unionsrecht oder im Recht der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall erfüllt sind. Erfasst sind sowohl Register, in die jedermann ohne Erfüllung weiterer Voraussetzungen Einsicht nehmen kann – in Deutschland etwa das Handels- oder Vereinsregister –, als auch solche, in die nur bei Vorliegen eines berechtigten Interesses Einsicht genommen werden kann, wie in Deutschland etwa das Grundbuch.

44 Zudem beschränkt Art. 49 Abs. 2 DSGVO die Übermittlung: Die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten dürfen nicht übermittelt werden. Ferner darf die Übermittlung, wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind. Durch diese Einschränkungen soll verhindert werden, dass praktisch das gesamte Register übermittelt und/oder in dem Register enthaltene Daten zu anderen Zwecken genutzt werden als zu dem Zweck, zu dem das Register eingerichtet ist.

5. Fazit

45 Bayerische öffentliche Stellen dürfen personenbezogene Daten nur unter engen Voraussetzungen an Empfänger in Drittländern oder an internationale Organisationen übermitteln. Sofern kein Angemessenheitsbeschluss der Europäischen Kommission vorliegt, sind vorrangig geeignete Garantien vorzusehen, um die personenbezogenen Daten der bayerischen Bürgerinnen und Bürger angemessen zu schützen. Hierbei sind auch technisch-organisatorische Maßnahmen in den Blick zu nehmen.

[1] Vgl. Art. 1 Beschluss des gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 2018 zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäß Artikel 101) des EWR-Abkommens, ABl. L 183 vom 19. Juli 2018, S. 23.

[2] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, Internet: https://www.bsi.bund.de, Rubrik „Themen – IT-Grundschutz".

[3] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4. Mai 2016, S. 89.

[4] Dazu näher Bayerischer Landesbeauftragter für den Datenschutz, Die Datenschutz-Grundverordnung. Ein Überblick, unter II. und III., Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Informationsreihe – Überblick".

[5] Zur Auftragsverarbeitung Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Stand 4/2019, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Auftragsverarbeitung".

[6] Vgl. Bundestags-Drucksache 18/12611, S. 113 ff.

[7] Vgl. auch Europäischer Gerichtshof, Urteil vom 6. Oktober 2015, C-362/14, Rn. 68, noch zu Art. 25 Abs. 6 Richtlinie 95/46/EG.

[8] Europäischer Datenschutzausschuss, Referenzgrundlage für Angemessenheit, Stand 2/2018, WP 254 rev.01, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Internationaler Datenverkehr".

[9] Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, ABl. L 207 vom 1. August 2016, S. 1.

[10] Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18, Rn. 150 ff.

[11] Europäischer Gerichtshof, Urteil vom 6. Oktober 2015, C-362/14.

[12] Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA (2000/520/EG), ABl. L 215 vom 25. August 2000, S. 7, ber. ABl. L 115 vom 25. April 2001, S. 14.

[13] Personal Information Protection and Electronic Documents Act vom 13. April 2000, S. C. 2000, c. 5, Internet: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html (konsolidierte Fassung).

[14] Entscheidung der Kommission vom 20. Dezember 2001 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (2002/2/EG), ABl. L 2 vom 4. Januar 2002, S. 13.

[15] Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (2001/497/EG), ABl. L 181 vom 4. Juli 2001, S. 19.

[16] Entscheidung der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2004/915/EG), ABl. L 385 vom 29. Dezember 2004, S. 74.

[17] Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (2010/87/EU), ABl. L 39 vom 12. Februar 2010, S. 5, geändert durch Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. Dezember 2016 zur Änderung der Entscheidung 2001/497/EG und des Beschlusses 2010/87/EU über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer sowie an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. L 344 vom 17. Dezember 2016, S. 100.

[18] Europäischer Gerichtshof, Urteil vom 16. Juli 2020, C-311/18, Rn. 122 ff.

[19] Näher Europäischer Datenschutzausschuss, Leitlinien 4/2018 zur Akkreditierung von Zertifizierungsstellen gemäß Artikel 43 der Datenschutz-Grundverordnung (2016/679), Version 3.0, Stand 6/2019; ders., Guidelines

1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, Version 3.0, Stand 6/2019, jeweils Internet: https://edpb.europa.eu, Rubrik „Unsere Arbeit und Hilfsmittel – Allgemeine Leitlinien – DSGVO: Leitlinien, Empfehlungen, bewährte Verfahren".

[20] Siehe auch Europäischer Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, Stand 5/2018, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Internationaler Datenverkehr".

[21] Dazu Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung".

[22] Vgl. Europäischer Datenschutzausschuss, Guidelines 5/2020 on consent under Regulation 2016/679, Version 1.1, Stand 5/2020, Fn. 47, Internet: https://edpb.europa.eu, Rubrik „Unsere Arbeit und Hilfsmittel – Allgemeine Leitlinien – DSGVO: Leitlinien, Empfehlungen, bewährte Verfahren".

[23] Vgl. Europäischer Datenschutzausschuss, Guidelines 5/2020, S. 31.