Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?

Herausgegeben vom
Landesbeauftragten für den Datenschutz und die Informationsfreiheit Dr. Stefan Brink
Mitautorinnen: Lena Mitsdörffer, persönliche Referentin des LfDI; Johanna Krieger, Leitung Stabstelle Europa beim LfDI,
K. Vogt, Referentin Stabstelle Europa beim LfDI
Lautenschlagerstraße 20, 70173 Stuttgart
Telefon: 0711/615541-0
Telefax: 0711/615541-15
https://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
Mastodon: https://bawü.social/@lfdi
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

4. Auflage, September 2021. Aktualisierung unter Berücksichtigung des Durchführungsbeschlusses (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.

Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?

Hinweise des LfDI
und Festlegung seines weiteren Vorgehens
zum Urteil des Europäischen Gerichtshofs
(EuGH) vom 16. Juli 2020, Rechtssache C-311/18
(„Schrems II“)

I Worum geht's?

Hintergrund

Ein Rechtsstreit zwischen einer Privatperson (Maximilian Schrems) und der irischen Aufsichtsbehörde über die Übermittlung seiner personenbezogenen Daten durch Facebook Irland zum Mutterkonzern von Facebook in die USA.

Kernaussagen

1. Die **Datenschutz-Grundverordnung (DS-GVO)** findet auf die Übermittlung personenbezogener Daten in ein Drittland auch in solchen Fällen **Anwendung**, in denen es aus Gründen der nationalen Sicherheit oder Verteidigung zu einem Zugriff durch Geheimdienste dieses Landes kommt.

   Die Ausnahmen des Art. 2 Abs. 2 a, b, d der DS-GVO gelten nur für die Mitgliedstaaten der EU.

2. Das **sogenannte „Privacy Shield"**, ein Angemessenheitsbeschluss der Kommisssion nach Art. 45 DS-GVO (2016/1250 vom 12.07.2016, noch zur Datenschutz-Richtlinie 95/46/EC), mit dem diese 2016 beschlossen hatte, dass die USA unter bestimmten Umständen ein angemessenes Schutzniveau für die Daten natürlicher Personen bieten und so die Übermittlung von Daten in die USA allgemein ermöglicht hatte, **ist ab sofort ungültig.**

   Aufgrund der Befugnisse der US-Geheimdienste und der Rechtslage in den USA kann ein angemessenes staatliches Datenschutz-Niveau (Art. 45 DS-GVO) nicht sichergestellt werden (u. a.):

   - Section 702 des Foreign Intelligence Surveillance Act (FISA) sieht keine Beschränkungen der Überwachungsmaßnahmen der Geheimdienste und keine Garantien für Nicht-US-Bürger vor,
   - Presidential Policy Directive 28 (PPD-28) gibt Betroffenen keine wirksamen Rechtsbehelfe gegen Maßnahmen der US-Behörden und sieht keine Schranken für die Sicherstellung verhältnismäßiger Maßnahmen vor,
   - der im Privacy Shield vorgesehene Ombudsmann hat keine genügende Unabhängigkeit von der Exekutive; er kann keine bindenden Anordnungen gegenüber den Geheimdiensten treffen.

   Maßstab der Feststellung des EuGH, dass die staatlichen Überwachungsmaßnahmen der USA unverhältnismäßig sind, ist die EU-Grundrechte-Charta.

3. **Die von der Kommission im Jahr 2010 beschlossenen Standardvertragsklauseln** reichen für Datenübermittlungen in Drittländer ohne zusätzliche Maßnahmen nicht mehr aus.

   Per Durchführungsbeschluss (EU) 2021/914 vom 4. Juni 2021 hat die EU-Kommission nun jedoch die neuen Standardvertragsklauseln (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914)
   (Standarddatenschutzklauseln) für die Übermittlung personenbezogener Daten an Drittländer gemäß der DS-GVO veröffentlicht.[1] (Siehe dazu Ausführungen unter III.)

   Es muss ein Schutzniveau für die personenbezogenen Daten sichergestellt sein, das dem in der Europäischen Union entspricht.

   - Auszulegen im Lichte der EU-Grundrechte-Charta und im Hinblick auf Art. 46 Abs. 1 DS-GVO: **geeignete Garantien** des Verantwortlichen oder des Auftragsverarbeiters, **durchsetzbare Rechte** und **wirksame Rechtsbehelfe** für die betroffenen Personen,
   - Hier sind nicht nur die vertraglichen Beziehungen zwischen Datenexporteur und Datenimporteur relevant, sondern auch die Zugriffsmöglichkeit auf die Daten durch Behörden des Drittlandes und das Rechtssystem dieses Landes insgesamt (Gesetzgebung und Rechtsprechung, Verwaltungspraxis von Behörden).

4. *Ist ein solches angemessenes Schutzniveau nicht sichergestellt,* ***muss die Aufsichtsbehörde für den Datenschutz die Datenübermittlung aussetzen oder verbieten****, wenn der Schutz nicht durch andere Maßnahmen hergestellt werden kann.*

[1] Außerdem wurden Standardvertragsklauseln nach Art. 28 Abs. 7 DS-GVO (als Alternative zur individuellen Auftragsverarbeitungsvereinbarung, d. h. Datenverkehr ausschließlich innerhalb der EU) veröffentlicht: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915

II Wen betrifft diese Entscheidung?

Zwar entfaltet das Urteil des EuGH zunächst nur inter partes-Wirkung, ist also erst einmal nur für das vorlegende irische Gericht bindend. **Faktisch** entfaltet es aber bereits jetzt **Bindungswirkung für alle Behörden und Gerichte der Mitgliedstaaten**, die sich mit derselben Auslegungsfrage beschäftigen und die DS-GVO unter Berücksichtigung der Rechtsprechung des EuGH auslegen und anwenden müssen.

Erklärt der EuGH einen Gemeinschaftsrechtsakt (wie das **Privacy Shield**) für ungültig, sind daran alle Gerichte und Behörden in allen Mitgliedstaaten gebunden und demnach auch alle dem EU-Recht unterworfenen **Unternehmen** (erga omnes-Wirkung).

Insofern betrifft die Entscheidung alle öffentlichen Stellen oder Unternehmen, die Daten in die USA transferieren, insbesondere, wenn sie die Übermittlung dabei bisher auf das Privacy Shield gestützt haben, aber auch, wenn sie dafür die alten Standardvertragsklauseln von 2010 genutzt haben (wie genau, dazu sogleich).

Beispiele (nicht abschließend):

- Sie stehen in Handelsbeziehung mit Unternehmen, die einen Sitz in den USA haben und tauschen mit diesen personenbezogene Daten über Kunden (Lieferadressen, Beschwerden, Bestellungen etc.) oder Ihre Beschäftigten (Verträge, Netzwerke, etc.) aus.
- Sie speichern Daten in einer Cloud, die von einem Unternehmen in den USA außerhalb der EU gehostet wird.
- Sie nutzen ein Videokonferenzsystem eines US-amerikanischen Anbieters, der Daten der Teilnehmenden erhebt und in die USA übermittelt.

Gleichzeitig enthält das Urteil allgemeine Aussagen zur Nutzung der alten Standardvertragsklauseln von 2010 für eine Übermittlung von Daten in Drittländer, sodass **auch alle öffentlichen Stellen oder Unternehmen, die Daten nicht in die USA, sondern in ein anderes Drittland übermitteln, von der Entscheidung betroffen sind.**

Beispiel: Sie übermitteln Daten in das Vereinigte Königreich oder nach Indien.

Die Auswirkungen der Gerichtsentscheidung sind daher **denkbar umfassend**.

III Was bedeutet die Entscheidung konkret? Was ist zu tun?

1. **Wenn Sie Daten in die USA übermitteln oder sich eines Auftragsverarbeiters bedienen, der Daten in die USA übermittelt:**

   - das **Privacy Shield** stellt **keine gültige Rechtsgrundlage** für die Übermittlung mehr dar, **trotzdem durchgeführte Datentransfers sind rechtswidrig und können Bußgelder und Schadensersatzforderungen nach sich ziehen**.
   - **eine Übermittlung auf Grundlage der alten Standardvertragsklauseln von 2010 ist bei Bestandsübermittlungen zwar denkbar**, wird die Anforderungen, die der EuGH an ein wirksames Schutzniveau gestellt hat, **jedoch nur in seltenen Fällen erfüllen**: Der Verantwortliche muss hier **zusätzliche Garantien** bieten, die einen Zugriff durch die US-amerikanischen Geheimdienste effektiv verhindern und so die Rechte der betroffenen Personen schützen; dies wäre etwa in folgenden Fällen denkbar:
     - **Verschlüsselung**, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann,
     - **Anonymisierung aller personenbezogenen Daten.**

Die Verwendung der alten Standardvertragsklauseln ist nur noch bis zum Ende der Übergangsfrist am 27.12.2022 zulässig. Dazu hatte der EuGH im Urteil „Schrems II" aber bereits festgestellt, dass die alten Standardvertragsklauseln alleine nicht genügen. Die alten Klauseln sind nur unter der Voraussetzung geeigneter Garantien nach Art. 46 Abs. 1 DS-GVO verwendbar.
Daher hatte der LfDI Baden-Württemberg in der Vorversion dieser Orientierungshilfe eine Ergänzung der Klauseln gefordert. Die Übergangsfrist wird in der Praxis also keine Erleichterung hinsichtlich des Erfordernisses geeigneter zusätzlicher Garantien bedeuten.

- **eine Übermittlung auf Grundlage der neu erlassenen Standarddatenschutzklauseln von 2021:**

  In diesen wird jedenfalls ein Teil der sich aus dem Schrems II-Urteil ergebenden Anforderungen adressiert.

  Die neuen Standarddatenschutzklauseln nach Artikel 46 Absatz 2 Buchstabe c) DS-GVO setzen sich aus allgemeinen Klauseln und modular aufgebauten Klauseln zusammen. Sie enthalten die folgenden vier Module für die Übermittlung…

  - **von Verantwortlichen an Verantwortliche (Modul 1)**
  - **von Verantwortlichen an Auftragsverarbeiter (Modul 2)**
  - **von Auftragsverarbeitern an Auftragsverarbeiter (Modul 3)**
  - **von Auftragsverarbeitern an Verantwortliche (Modul 4).**

Hinweis: Hier ist allerdings Obacht geboten. Klauseln 1, 2, 4 bis 7 sowie Teile von Klausel 3 gelten für alle vier Varianten. Bei den anderen Klauseln ist aber jeweils zu prüfen, ob sie für das Modul einschlägig sind und nur die passende Version aufzunehmen.

Betroffene sind gemäß Artikel 13 Absatz 1 Buchstabe f) DS-GVO schon über die Absicht des Verantwortlichen zu informieren, personenbezogene Daten in ein Drittland zu übermitteln. Vor der Übermittlung muss der Datenexporteur prüfen, ob das Datenschutzniveau im Drittland mit dem in der Europäischen Union vergleichbar ist.

Die **neue Klausel 14** der Standarddatenschutzklauseln sieht vor, dass zur Bestimmung des Datenschutzniveaus auch Gepflogenheiten im Bestimmungsdrittland herangezogen werden können, einschließlich Anforderungen zur Offenlegung personenbezogener Daten oder Maßnahmen, die öffentlichen Behörden den Zugang zu diesen Daten gestatten. Dies kann nach Fußnote 12 auch einschlägige und dokumentierte praktische Erfahrungen im Hinblick darauf umfassen, ob es bereits früher Ersuchen um Offenlegung seitens Behörden gab.

Hier ist jedoch in höchstem Maße Vorsicht geboten. Denn es ist kaum anzunehmen, dass ein Rückzug auf solche bloßen praktischen Erfahrungen den vom EuGH geforderten zusätzlichen Garantien genügt, die sicherstellen sollen, dass die Datenschutzvorschriften und die Rechte der betroffenen Personen auf eine der Verarbeitung innerhalb der Union angemessene Art und Weise beachtet werden. Datenexporteuren ist viel mehr zu raten, sich an den praktischen Beispielen zu möglichen zusätzlichen Garantien zu orientieren und diese zu implementieren, wie sie die Empfehlung des Europäischen Datenschutzausschusses in Anhang 2 enthält: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf.

Die neuen Standarddatenschutzklauseln setzen – jedenfalls zum Teil – einige der Forderungen um, die der LfDI aufgestellt hatte. Daher stellen die neuen Klauseln bereits eine Verbesserung dar und es empfiehlt sich, baldmöglichst auf die neuen Klauseln umzusteigen. **Allerdings rät der LfDI, die neuen Klauseln wie folgt zu ergänzen:**

- Klausel 15.1 a) der neuen SCC sieht die Pflicht des Datenimporteurs vor, nicht nur den Datenexporteur, sondern soweit möglich auch die betroffene Person unverzüglich über alle rechtlich bindenden **Aufforderungen einer Behörde zur Weitergabe der personenbezogenen Daten** oder über den Fall, dass eine Behörde direkten Zugang zu personenbezogenen Daten erhalten hat, **zu benachrichtigen** (der LfDI hatte die Information der Betroffenen als Ergänzung der alten Klausel 5d i empfohlen); Betroffene können aufgrund der Drittbegünstigungsklausel 3 a) vi) u. a. regelmäßige sachdienliche Informationen über eingegangene Behördenersuchen einfordern.

  Ist diese Informationsweitergabe anderweitig untersagt, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen, müssen Sie sich mit der Aufsichtsbehörde LfDI in Verbindung setzen und das weitere Vorgehen abklären; die Verpflichtung des Datenimporteurs für diese Fälle, regelmäßig dem Datenexporteur allgemeine Informationen über erhaltene Anfragen von Behörden zu unter diesem Vertrag verarbeitete personenbezogene Daten zur Verfügung zu stellen (insbesondere Anzahl der Anträge, Art der angefragten Daten, ersuchende Stelle), ist nun in Klausel 15.1 c) vorgesehen.

- Klausel 15.2. a) sieht die Verpflichtung des Datenimporteurs vor, **den Rechtsweg gegen eine Weitergabe von personenbezogenen Daten zu beschreiten** und die personenbezogenen Daten erst offenzulegen, wenn dies nach den geltenden Verfahrensregeln erforderlich ist. Der LfDI hatte die Verpflichtung als Ergänzung der alten Klausel 5 d empfohlen. In der neuen Klausel fehlt allerdings die Klarstellung, dass eine einstweilige Entscheidung nicht ausreicht. Daher empfiehlt der LfDI die Ergänzung der Klausel 15.2. a) durch die Verpflichtung des Datenimporteurs, die Offenlegung der personenbezogenen Daten gegenüber den jeweiligen Behörden zu unterlassen, bis er von einem zuständigen Gericht im Hauptsacheverfahren letztinstanzlich zur Offenlegung rechtskräftig verurteilt wurde; zudem sollte Klausel 15. 2. a) inklusive dieser Ergänzung in die Drittbegünstigungsklausel, ergänzend zu Klausel 3 a) vi) aufgenommen werden.

  Das gilt insbesondere, wenn das Recht des Drittlandes dem Datenimporteur Verpflichtungen auferlegt, die geeignet sind, vertraglichen Regeln, die einen geeigneten Schutz gegen den Zugriff durch staatliche Behörden vorsehen, zuwider zu laufen.

- **Ergänzung von Anhang Klausel 8.2** um die Verpflichtung des Datenimporteurs, soweit dieser ihm bekannt ist auch den Betroffenen von der Vergabe eines Verarbeitungsauftrags an einen **Unterauftragsverarbeiter** zu **benachrichtigen**; Aufnahme dieser Ergänzung in die Drittbegünstigungsklausel, ergänzend zu Klausel 3 ii).

- Eine **Übermittlung nach Art. 49 DS-GVO ist in Ausnahmefällen denkbar**; jedoch ist hier der **insgesamt restriktive Charakter dieser Vorschrift** zu beachten (vgl. dazu auch die Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 des Europäischen Datenschutzausschusses (EDSA) vom 25.05.2018, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_de):

- Wortlaut des Titels „Ausnahmen für bestimmte Fälle“: **Ausnahmecharakter von Artikel 49** als Abweichung vom Regelverbot der Übermittlung in Drittstaaten bei Nichtvorliegen eines angemessenen Datenschutzniveaus,

- für Art. 49 Abs. 1 UAbs. 1 b, c und e DS-GVO (für Vertrag oder zur Geltendmachung von Rechtsansprüchen erforderlich) zusätzlich: **Wortlaut EG 111**: **„gelegentlich“** erfolgende Datenübermittlungen, nicht systematisch wiederholend,
- **noch restriktiver: Art. 49 Abs. 1 UAbs. 2** für Fälle, in denen keine Ausnahme für bestimmte Fälle vorliegt (Übermittlung nicht wiederholt, nur eine begrenzte Zahl von betroffenen Personen, erforderlich für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen, kein Überwiegen des Interesses oder der Rechte und Freiheiten der betroffenen Person),
- **für Behörden** gelten zudem gem. Art. 49 Abs. 3 DS-GVO die Art. 49 Abs. 1 UAbs. 1 a, b und c sowie UAbs. 2 nicht bei Ausübung ihrer hoheitlichen Befugnisse.

2. **Wenn Sie Daten in ein anderes Drittland ohne angemessenes Datenschutzniveau übermitteln:**
   - Hier sollten Sie die Rechtslage in dem genannten Land überprüfen, insbesondere hinsichtlich der Zugriffsmöglichkeiten des Geheimdienstes und der dem Betroffenen zustehenden Rechte und Rechtsschutzmöglichkeiten
   - und auch hier zumindest die unter III. 1. genannten Ergänzungen der Standarddatenschutzklauselnaufnehmen sowie für die genannten zusätzlichen Garantien sorgen.

IV Wo und wie anfangen? / Checkliste

Sie sollten jetzt unverzüglich

- ✔ eine **Bestandsaufnahme** (Inventur) machen, in welchen Fällen Ihr Unternehmen/Ihre Behörde personenbezogene Daten in Drittländer **exportiert**; darunter können auch bloße Zugriffsmöglichkeiten von privaten oder öffentlichen Stellen in Drittstaaten auf bei Ihnen vorgehaltene Daten fallen (Schnittstellen, Abrufmöglichkeit, Fernwartung), ein „physischer" Export der Daten ist also nicht erforderlich.
- ✔ **sich mit Ihrem Dienstleister/Vertragspartner im Drittland in Verbindung setzen** und ihn über die Entscheidung des EuGH und deren Konsequenzen informieren.
- ✔ **Ihre Datenschutzerklärungen prüfen und anpassen, insbesondere im Hinblick auf Ihre Informationspflicht nach Art. 13 Abs. 1 f DS-GVO**: Danach sind die betroffenen Personen nicht nur über Ihre Absicht, die personenbezogene Daten an ein Drittland zu übermitteln, zu unterrichten, sondern auch über den Transfermechanismus – aktualisieren Sie Ihre Angaben (wird dort z. B. noch das Privacy Shield als Transfermechanismus benannt, ist dies zu streichen und die Erklärung entsprechend anzupassen).
- ✔ Ihre **Verzeichnisse der Verarbeitungstätigkeiten** entsprechend **prüfen und anpassen**
- ✔ **alle Auftragsverarbeiter**, die personenbezogene Daten unter dem Privacy Shield in die USA übermitteln oder dort verarbeiten, **umgehend** schriftlich/per E-Mail (wie im entsprechenden Vertrag gefordert) **anweisen, die Übermittlung personenbezogener Daten in die USA mit sofortiger Wirkung auszusetzen**, bis ihr Auftragsverarbeiter bzw. dessen Unterauftragnehmer dort im Einzelfall ein der DS-GVO entsprechendes Datenschutzniveau, etwa durch Einsatz alternativer Verarbeitungs- und Transfermechanismen, sichergestellt hat.
- ✔ **sich über die Rechtslage im Drittland informieren** (Datenschutzgesetze des Drittlandes; Zugriffsmöglichkeiten staatlicher Stellen einschließlich der Geheimdienste auf Ihre Daten; Ihnen, dem Datenimporteur und dem Betroffenen zustehende Rechte und Rechtsschutzmöglichkeiten; Rechtsprechung und Behördenpraxis im Drittland mit Bezug zum Datenschutzniveau); öffentliche Stellen wie die Datenschutz- Aufsichtsbehörden, der Europäische Datenschutz-Ausschuss (EDSA), die EU-Kommission oder das Auswärtige Amt sollten dazu jeweils Hilfestellungen geben können.

✔ **überlegen, ob Sie einen Transfer von Daten in Drittländer nicht dadurch vermeiden können**, dass Sie

- nur Dienste nutzen, die keine Daten in ein Drittland übertragen, oder
- die vertragliche Vereinbarung treffen, dass keine Datenübertragung in ein Drittland vorgenommen wird,
- die Daten verschlüsseln und allein Zugriff auf den Schlüssel haben.

  Dabei ist wiederum die gesamte Rechtslage des Drittlands in den Blick zu nehmen (etwa innerstaatliche Regelungen zum Zugriff auf Datenbestände außerhalb des eigenen Hoheitsgebietes, vgl. US-Cloud Act, dazu https://edps.europa.eu/sites/edp/files/publication/19-07-10_edpb_edps_cloudact_annex_en.pdf).

✔ **überprüfen, ob es für das Drittland einen Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DS-GVO gibt**

Für die USA wurde dieser nun für ungültig erklärt, aber etwa für Argentinien, Kanada, Japan, Neuseeland, die Schweiz oder das Vereinigte Königreich besteht diese Grundlage noch, siehe eine ausführliche Liste hier: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

✔ **überprüfen, ob Sie die von der Kommission beschlossenen Standardvertragsklauseln für das jeweilige Land nutzen können (Art. 46 Abs. 2c DS-GVO)** – diese sind abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914

Eine Übermittlung von Daten mithilfe der alten Standardvertragsklauseln von 2010 ist in die USA nur mithilfe zusätzlicher Garantien (z.B. Verschlüsselung und Anonymisierung, s. o.) möglich. Dies hilft aus Sicht des LfDI derzeit jedoch nur in einer eng begrenzten Zahl von Fallkonstellationen und stellt daher keine Lösung für die Mehrzahl der Datentransfers in die USA dar.
Fehlt es an wirksamen zusätzlichen Garantien sollten Sie, um wenigstens Ihren Willen zu rechtskonformem Handeln zu demonstrieren und zu dokumentieren, **Kontakt mit dem jeweiligen Empfänger der Daten aufnehmen**.

- Die Forderung des LfDI, dass die betroffene Person, die durch eine Verletzung der in Klausel 3 genannten Pflichten durch eine Partei oder den Unterauftragsverarbeiter Schaden erlitten hat, berechtigt ist, **nicht nur vom Datenexporteur Schadenersatz** für den erlittenen Schaden zu erlangen, **sondern auch vom Datenimporteur**, ist in der neuen Klausel 12 b) vorgesehen.

- Die Aufnahme des in Anhang 2 der alten Standardvertragsklauseln von 2010 genannten Beispiels für eine Entschädigungsklausel ist in der neuen Klausel 12 d) weitestgehend enthalten.
- In den neuen Standarddatenschutzklauseln fehlt **die Verpflichtung des Datenimporteurs, den Betroffenen verschuldensunabhängig** von allen **Schäden** freizustellen, die **durch den Zugriff von Stellen seines Staates** auf die Daten der Betroffenen entstehen. Der LfDI empfiehlt, diese Verpflichtung aufzunehmen.

✔ **überprüfen**, ob Sie sich auf v**erbindliche interne Datenschutzvorschriften gemäß Artikel 47 (Binding Corporate Rules BCRs)** berufen können; auch hier können – wie im Falle der Standardvertragsklauseln – zusätzliche Garantien erforderlich sein. Wesentliche Änderungen der BCR müssen der zuständigen Aufsichtsbehörde zur erneuten Genehmigung vorgelegt werden.

✔ **überprüfen**, ob als letztes Mittel die Übermittlung von Daten nach der **Ausnahmevorschrift des Art. 49 DS-GVO** in Betracht kommt. Dies kann insbesondere der Fall sein bei Datenübermittlungen im Konzern oder bei Einzelvertragsbeziehungen. Hier wäre zu prüfen, ob der restriktive Charakter der Norm der Übermittlung nicht entgegensteht.

✔ überprüfen, ob Sie alle Prüfungsschritte und Folgerungen **dokumentiert** haben und **nachweisen** können (Art. 5 Abs. 2 DS-GVO).

Im Zentrum des weiteren Vorgehens des LfDI Baden-Württemberg wird die Frage stehen, ob es neben/mit dem von Ihnen gewählten Dienstleister/Vertragspartner nicht **auch zumutbare Alternativangebote ohne Transferproblematik** gibt. Wenn Sie uns nicht davon überzeugen können, dass der von Ihnen genutzte Dienstleister/Vertragspartner mit Transferproblematik kurz- und mittelfristig unersetzlich ist durch einen zumutbaren Dienstleister/Vertragspartner ohne Transferproblematik, dann wird der Datentransfer vom LfDI Baden- Württemberg **untersagt** werden.

Uns ist bewusst, dass mit dem Urteil des EuGH u.U. extreme Belastungen für einzelne Unternehmen einhergehen können. Der LfDI wird sein weiteres Vorgehen am Grundsatz der Verhältnismäßigkeit ausrichten.

Wir werden die Entwicklung weiter beobachten und unsere Positionen dementsprechend laufend überprüfen und fortentwickeln.

NOTIZEN

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg