Stellungnahme zu den datenschutzrechtlichen Folgen des Austritts des Vereinigten Königreichs aus der Europäischen Union („Brexit“)

Autor: Eva Schlehahn - EDV-Unternehmensberatung Floß GmbH
Datum: 15.01.2021

1 Kurzüberblick (Management Summary)

Mit Ablauf des 31.12.2020 wurde der Austritt des Vereinigten Königreichs, der sogenannte „Brexit“, vollzogen. Nach langen Verhandlungen konnte gerade rechtzeitig vor Jahresablauf mit einer Einigung über ein Handels- und Kooperationsabkommen noch das „No-Deal“ Szenario abgewendet werden. Noch fehlt jedoch die parlamentarische Ratifizierung des Austrittabkommens, welche bis zum 28. Februar erfolgen muss. In der Theorie könnten die Parlamente der beteiligten Partien noch die Ratifizierung des Abkommens ablehnen. In der Praxis ist dies allerdings nicht sehr wahrscheinlich. Es ist eher davon auszugehen, dass das vereinbarte Abkommen Bestand haben wird.

Mit dem Austritt und dem Abkommen ergeben sich in bestimmten Konstellationen datenschutzrechtliche Folgen für Unternehmen in Europa. Der Brexit ist aus Datenschutzsicht für europäische Unternehmen dann relevant, wenn

- diese eine (selbstständige/unselbstständige) Niederlassung in Großbritannien haben,
- eine Übermittlung personenbezogener Daten (z.B. von Kund*innen, Nutzer*innen oder Arbeitnehmer*innen) nach Großbritannien erfolgt oder in Großbritannien ansässige Unternehmen Zugriff auf solche Informationen gewähren,
- Dienstleister aus dem Vereinten Königreich genutzt werden (wie etwa Lieferservices),
- in Großbritannien ansässige Online-Dienste genutzt werden (z.B. Cloud/SaaS-Dienste wie z. B. Marketing & Analysetools, Social Media oder Recruitingdienste).

Unternehmen, bei denen grenzüberschreitende Datenübermittlung nach Großbritannien stattfindet, haben infolge des Abkommens eine Schonfrist erhalten. Denn eigentlich würde Großbritannien in datenschutzrechtlicher Hinsicht seit dem Austritt als Drittland im Sinne der DSGVO gelten. Das vereinbarte Handels- und Kooperationsabkommen sieht aber vor, dass ab 1.1.2021 der Drittlandstatus für mindestens vier, gegebenenfalls automatisch verlängerbar auf sechs Monate, nicht anzuwenden ist. Das bedeutet, dass eine grenzüberschreitende Datenübermittlung unter unveränderten Bedingungen noch mindestens bis zum 30. April 2021, eventuell sogar bis zum 30. Juni 2021, möglich ist.

Allerdings ist diese Schonfrist keine dauerhafte Lösung für grenzüberschreitende Datentransfers. Vor allem ist für die Zeit danach unklar, ob Großbritannien als Drittland einen Angemessenheitsbeschluss der Europäischen Kommission erhalten wird. Aufgrund der Rechtslage in Großbritannien mit weitreichenden Überwachungsbefugnissen der Sicherheitsbehörden, welche den Datenschutz schwächen, ist jedoch zweifelhaft, ob ein solcher Angemessenheitsbeschluss ergehen wird. Zudem ist der Zeitrahmen für den rechtzeitigen Erlass eines solchen Beschlusses denkbar knapp.

Sollte es keinen Angemessenheitsbeschluss geben, so müssen Verantwortliche und Auftragsverarbeiter, die weiterhin Daten nach Großbritannien übermitteln wollen, aktiv dafür sorgen, dass diese nach der DSGVO rechtskonform erfolgt. Das erfordert die Gewährleistung

eines angemessenen Datenschutzniveaus mit geeigneten Garantien, damit die Datenübermittlung rechtlich zulässig ist bzw. bleibt (vgl. EuGH - Urteil vom 16. Juli 2020 / Az. C-311/8).

Unsere Empfehlung ist, dass Unternehmen eine Vorgehensweise anwenden, wie wir sie im letzten Jahr schon aufgrund des EuGH-Urteils im Juli 2020 (Az. C-311/8, sog. „Schrems II" Urteil vom 16.7.2020) empfohlen haben. **Sämtliche personenbezogenen Verarbeitungen des Unternehmens und die dazugehörigen bestehenden Verträge sollten überprüft werden. Dabei sollten die folgenden Punkte im Verlauf der Prüfung adressiert und DSGVO-konform gelöst werden:**

- **Prüfung**, ob bei Verfahren **Datenübermittlungen** nach Großbritannien stattfinden bzw. in der vorliegenden Form stattfinden müssen.
- **Identifizierung der Rechtsgrundlagen** für die Datenübermittlung und Kontrolle im Hinblick auf deren Gültigkeit (Artt. 44 ff. DSGVO) auch nach Ablauf der Schonfrist. Nachfolgende Grundvoraussetzungen sollten geschaffen werden:
- Bei Bedarf **Grundlagen für die Übermittlung im Sinne v. Artt. 44 ff. DSGVO umstellen bzw. anpassen**.
    - Sofern geeignete Garantien erforderlich sind, können dies zum Beispiel Binding Corporate Rules (BCR), die EU-Standardvertragsklauseln der EU-Kommission, genehmigte Verhaltensregeln und genehmigte Zertifizierungsmechanismen sowie individuell vertraglich ausgehandelte Klauseln sein. Am einfachsten wird es für die meisten Unternehmen sein, fortan die EU-Standardvertragsklauseln einschließlich zu verwenden. Reine Auftragsverarbeitungsverträge gem. Artt. 28, 29 DSGVO reichen nicht mehr aus.
    - Sind keine der in Art. 46 DSGVO genannten Garantien anwendbar, so sollten noch die in Art. 49 DSGVO genannten Ausnahmen (z.B. für Einwilligung der Betroffenen oder Erforderlichkeit der Datenübermittlung zu Erfüllung von Verträgen) geprüft werden.
    - Für die Überprüfungen aktiv Informationen zu den Garantien einholen. So sollte z.B. bei Verwendung der Standardvertragsklauseln die britischen Dienstleister gefragt werden, welche ergänzenden Garantien zu diesen Klausen bereitgestellt werden.
- **Anpassung der Datenschutzerklärungen für Betroffene.**
    - Den Informationspflichten zur Datenübermittlung in ein Drittland nach Art. 13 Abs. 1 lit. f) + Art. 14 Abs. 1 lit. f) DS-GVO muss genügt werden. Es sollte transparent dargestellt werden, welche personenbezogenen Daten auf Grundlage welcher Garantien zu welchem Zweck in ein Drittland übermittelt werden.
    - Hierbei kann es sein, dass es nicht reicht, einfach nur die Datenschutzerklärung der Firmenwebseite anzupassen. Vielmehr muss die Information je nach betroffenem Verfahren gegenüber allen Betroffenen erfolgen (Arbeitnehmer*innen, Kund*innen und Nutzer*innen, etc.…).

- **Anpassung von Einwilligungserklärungen für Betroffene.**
  - Basiert die Datenverarbeitung auf einer Einwilligung (n. Artt. 7, 8 DSGVO), so muss auch eine **Anpassung der Betroffeneninformation** erfolgen. Es muss über die Datenübermittlung nach Großbritannien und über eventuelle bestehende Risiken aufgeklärt werden. Die Information muss auch die relevanten Rechtsgrundlagen und Garantien enthalten.
- **Anpassung von Auskünften gegenüber Betroffenen.**
  - Bei der Auskunftserteilung muss ebenfalls nach Art. 15. Abs. 1 lit. c) + Abs. 2 DSGVO über die Datenübermittlung in ein Drittland informiert werden. Dabei sind die Empfänger, die verbundenen Rechtsgrundlagen und die Garantien zu benennen.
- Erforderlichkeitsprüfung (Schwellwertanalyse) für die Durchführung einer **Datenschutz-Folgenabschätzung** in den betroffenen Verfahren. Ebenso ist eine Überprüfung bereits durchgeführter DSFA erforderlich, ob diese angepasst werden müssen.

Nebst diesen oben benannten Aspekten sollten betroffene Unternehmen aktiv den Prozess für den Angemessenheitsbeschluss der Europäischen Kommission verfolgen und bei Bedarf entsprechend reagieren. Ebenso muss geklärt sein, welche Datenschutzaufsichtsbehörden nun federführend für das jeweilige Unternehmen zuständig sind. Britische Unternehmen, die in der EU tätig sein wollen, müssen weiterhin klären, ob sie einen Vertreter in der EU für die dortigen Betroffenen und Aufsichtsbehörden bestellen müssen.

Im nachfolgenden Abschnitt werden die datenschutzrechtlichen Folgen des Brexits im Detail dargestellt. Im Anschluss daran finden sich im Annex die relevanten Normen der DSGVO.

Die Unternehmensberatung Floß GmbH unterstützt ihre Kunden bei den anfallenden Aufgaben sehr gerne. Gegebenenfalls ergibt sich im Laufe der Prüfung, dass zusätzlich noch die Sachkunde einer spezialisierten Kanzlei erforderlich wird. Wir können dann geeignete Kanzleien empfehlen, mit denen wir auf Wunsch in Kooperation zusammenarbeiten, um das beste Ergebnis für unsere Kunden zu erzielen.

2 Detaildarstellung der datenschutzrechtlichen Folgen des Brexits

Mit dem Handels- und Kooperationsabkommen zwischen der EU und Großbritannien[1] wurde auch eine Einigung hinsichtlich der zu geltenden datenschutzrechtlichen Bestimmungen für eine bestimmte Zeit erzielt.

Zunächst ist festgeschrieben, dass Großbritannien hinsichtlich der grenzüberschreitenden Übermittlung personenbezogener Daten für die Dauer eines festgelegten Zeitraums nicht als Drittland im Sinne des Unionsrechts gelten soll.[2] Der benannte Zeitraum ist hierbei definiert mit vier Monaten, automatisch verlängerbar um weitere zwei Monate vorbehaltlich etwaiger Einwände der Parteien.[3]

Diese Schonfrist gilt jedoch nur dann, wenn Großbritannien in dieser Zeit keine signifikanten Änderungen an seinen eigenen Datenschutzreglungen vornimmt, die von der DSGVO divergieren.[4] Ferner verpflichten sich die Vertragsparteien des Brexit generell, bestimmte Einschränkungen des grenzüberschreitenden Datenverkehrs zu unterlassen, um den Handel in der digitalen Wirtschaft zu erleichtern. Es wird die Überprüfbarkeit der Einhaltung dieser Verpflichtungen eingeräumt.[5]

Darüber hinaus erkennen beide Vertragsparteien das Recht Einzelner auf den Schutz ihrer personenbezogenen Daten und ihrer Privatsphäre an, verbunden mit dem Bekenntnis zu hohen Schutzstandards in der Hinsicht. Es besteht die gegenseitige Verpflichtung, die jeweils andere Partei über Maßnahmen mit Auswirkungen auf den Schutz der personenbezogenen Daten zu informieren.[6]

Das vereinbarte Abkommen tritt ab dem 1. Januar 2021 in Kraft, eine Ratifizierung durch die Parlamente muss bis zum 28. Februar 2021 erfolgen.[7] Eine Weiterübertragung des Datentransfer-Abkommens durch Großbritannien an andere Handelspartner, wie etwa die Vereinigten Staaten, ist nicht vorgesehen.

---

[1] Handels- und Kooperationsabkommen zwischen der Europäischen Union und der Europäischen Atomgemeinschaft einerseits und dem Vereinten Königreich Großbritannien und Nordirland andererseits vom 31.12.2020 (L 444/14).
[2] Teil Sieben: Schlussbestimmungen des Abkommen - Artikel FINPROV.10A, Abs. 1: Übergangsbestimmung für die Übermittlung personenbezogener Daten an das Vereinigte Königreich, Seite 468.
[3] Ibidem, Artikel FINPROV.10A, Absatz 4.
[4] Ibidem, Artikel FINPROV.10A, Absatz 5.
[5] Teil Zwei: Handel, Verkehr, Fischerei und sonstige Regelungen im Abkommen - dort Titel III: Digitaler Handel, Kapitel 2: Datenfluss und Schutz personenbezogener Daten, Artikel DIGIT.6 Grenzüberschreitender Datenverkehr, Seite 145.
[6] Teil Zwei: Handel, Verkehr, Fischerei und sonstige Regelungen, dort Titel III: Digitaler Handel,
Kapitel 2: Datenfluss und Schutz personenbezogener Daten, Artikel DIGIT.7 Schutz personenbezogener Daten und der Privatsphäre, Seite 145.
[7] Teil Sieben: Schlussbestimmungen, Artikel FINPROV.11: Inkrafttreten und vorläufige Anwendung, Seite 470.

Die vereinbarte Schonfrist von vier bzw. max. sechs Monaten ist jedoch keine dauerhafte Lösung für den grenzüberschreitenden Datenverkehrt zwischen Großbritannien und der EU.

Bereits im Januar 2018 hatte die Europäische Kommission in einer Pressemitteilung klargestellt, dass Großbritannien mit dem Brexit den Status eines Drittlandes im Sinne der europäischen Datenschutzgrundverordnung (DSGVO) erlangen wird.[8] Bei Drittländern außerhalb der Europäischen Union besteht zunächst stets die Grundannahme, dass dieses Land kein angemessenes Datenschutzniveau, wie es die DSGVO erfordert, bietet. Dies hindert faktisch den freien, grenzüberschreitenden Datenfluss. Anderes jedoch gilt stets dann, wenn es einen sogenannten Angemessenheitsbeschluss der Europäischen Kommission im Sinne von Art. 45 Abs. 3 DSGVO gibt.

Ein Angemessenheitsbeschluss für ein bestimmtes Drittland bedeutet, dass die Kommission festgestellt hat, dass die Datenschutzgesetze dieses Landes einen dem Europäischen Datenschutzrecht vergleichbaren Schutz für die personenbezogenen Daten von Individuen bieten. Existiert also ein Angemessenheitsbeschluss, so ist die Voraussetzung dafür gegeben, dass personenbezogene Daten (mit einer einfachen Auftragsverarbeitung unter Einhaltung der sonstigen DSGVO Regeln) ohne weitere Voraussetzungen grenzüberschreitend übermittelt werden dürfe. Es erfolgt somit eine Gleichstellung von dem anerkannten Drittland mit den EU-Ländern. Bisher haben eine Reihe von Ländern den Status eines Drittlandes mit Angemessenheitsbeschluss erlangt, wie zum Beispiel die Schweiz, Jersey, Guernsey, Neuseeland und seit neustem auch Japan. Der aktuelle Stand zu den Angemessenheitsbeschlüssen kann hier eingesehen werden: https://dsgvo-gesetz.de/themen/drittland/.

Die Erlangung eines Angemessenheitsbeschlusses ist definitiv für Großbritannien die beste Möglichkeit, weiterhin einen reibungslosen Datenfluss zu gewährleisten. Die Frage ist jedoch, wie groß die Chance ist, dass ein solcher seitens der Europäischen Kommission ergeht. Ein Angemessenheitsbeschluss setzt voraus, dass ein der EU vergleichbares Schutzniveau für die personenbezogenen Daten von Personen im Drittland besteht. Der wichtigste Faktor für die Beurteilung durch die Kommission wird sein, wie Großbritannien mit Angelegenheiten der Rechtsstaatlichkeit, der Einhaltung internationaler Menschenrechtsnormen und -standards sowie dem Recht der Bürger auf einen wirksamen Rechtsbehelf im Rahmen von Polizei, Justiz und nationaler Sicherheit umgeht.

Die britische Regierung hat ein neues Datenschutzgesetz (Data Protection Act 2018) erlassen, das sich sehr eng an die DSGVO anlehnt, um in Zukunft eine Angemessenheitsentscheidung der Europäischen Kommission zu erhalten. Schedule 2 dieses Gesetzentwurfs sieht jedoch recht weitreichende Ausnahmen von den Bestimmungen der DSGVO für personenbezogene

[8] Siehe die Pressemitteilung der Europäischen Kommission vom 9. Januar 2018: “Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection”, verfügbar unter: http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245

Daten vor. Solche Ausnahmen betreffen Datenverarbeitungen z. B. zum Zwecke der Verbrechensverhütung oder -aufdeckung und der damit verbundenen Risikobewertung. Dabei können auch private Akteure involviert sein, die in diesem Bereich als Outsourcing-Dienstleister fungieren.[9] Diese Ausnahmen könnten Auswirkungen darauf haben, ob sich die Kommission entschließt, einen Angemessenheitsbeschluss zu erlassen oder nicht.

Gerade im Hinblick auf die Aspekte der nationalen Sicherheit, Vorratsdatenspeicherung und Überwachungsbefugnisse der Polizei und Geheimdienste könnte dies kritisch sein. Diese Befugnisse wurden im Jahr 2016 bereits deutlich erweitert, als die sogenannte „Investigatory Powers Bill“[10] erlassen wurde. Dies ist ein Rechtsrahmen, der auf dem Data Retention and Investigatory Powers Act (DRIPA) aufbaut. Nach jahrelangem Rechtsstreit erklärte das britische Berufungsgericht jedoch im Januar 2018 DRIPA für rechtswidrig, da die Menschenrechte von britischen und EU-Bürgern gleichermaßen verletzt wurden. Dies bedeutet, dass auch die Investigatory Powers Bill geändert werden muss.[11] Ferner mag in Bezug auf die polizeilichen Befugnisse der britische „e-Evidence“ Deal mit den USA eine Rolle für die Kommission spielen.

Diese weitreichenden Behördenbefugnisse sind auch deshalb ein Problem, da die britische Gesetzgebung nicht mehr europäischer Kontrolle bzw. europäischen Rechtsbehelfen, wie etwa vor dem EuGH, unterliegt. Es droht ein mangelnder Rechtsschutz für EU-Bürger. Deswegen besteht das Risiko, dass die Kommission Großbritannien im Hinblick auf Datenschutz für ebenso unsicher wie die USA hält und deshalb kein Angemessenheitsbeschluss ergehen kann.

Zurzeit ist unklar, wie groß die Chancen des Vereinigten Königreiches sein werden, einen Angemessenheitsbeschluss zu erhalten. Zweifellos wird der politische Druck groß sein, einen solchen trotz der geltenden Rechtslage zu erlassen. Letztlich läuft es auf die Frage hinaus, ob die Europäische Kommission den politischen Willen hat, einen Angemessenheitsbeschluss zu verweigern oder nicht. Soll ein Angemessenheitsbeschluss jedoch erfolgen, so ist zusätzlich noch die Frage, ob dieser rechtzeitig vor Ablauf der Schonfrist ergeht. Bis dato dauert die schnellste Beschlussfassung der Kommission (im Fall von Argentinien) achtzehn Monate.

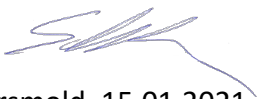
Wird entgegen der rechtlichen Bedenken Angemessenheit festgestellt, so ist zu erwarten, dass dies von Datenschutzaufsichtsbehörden, Bürgerrechtsverbänden oder von Betroffenen direkt angegriffen werden wird. Letztlich würden bei einer Vorlage vor dem EuGH dieselben Gesichtspunkte zum Tragen kommen, die bereits im „Schrems II“ Urteil des EuGHs eine Rolle gespielt haben. Großbritannien wird sich dann der bestehenden nationalen Überwachungsgesetzgebung an dem in diesem Urteil aufgestellten Maßstäben messen lassen müssen.

[9] Siehe den Text des UK Data Protection Act 2018, Schedule 2, verfügbar unter: https://www.legislation.gov.uk/ukpga/2018/12/contents.
[10] https://publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf.
[11] UK Court of Appeal (Civil division), Case No. C1/2015/2612 & 2613 SSHD v Watson & Others.

Unabhängig davon, ob ein Angemessenheitsbeschluss der Europäischen Kommission ergeht oder nicht, fällt das Vereinte Königreich aus dem europäischen Datenschutzregime heraus. Dies ist für Unternehmen vor allem auch im Hinblick auf den sogenannten One-Stop-Shop relevant. Dies ist eine Regelung, die innerhalb der Europäischen Union dazu führt, dass es in Datenschutzbelangen stets eine federführende Aufsichtsbehörde gibt., um bürokratische Hürden abzubauen. Da diese Regelung nicht mehr für Großbritannien anwendbar ist, könnte dies dazu führen, dass sich Unternehmen nun gegenüber mehreren Datenschutzaufsichtsbehörden, nämlich einer britischen und einer europäischen, verantworten müssen. Dies bedeutet für die Wirtschaft insgesamt ein höheres (nämlich doppeltes) Bußgeldrisiko, etwa im Falle von Datenschutzverstößen.

Verantwortliche und Auftragsverarbeiter sollten nun aktiv werden, um sich in datenschutzrechtlicher Hinsicht für jeden eventuellen Fall zu rüsten. Dies fängt mit der **Identifizierung der nun zuständigen federführenden Aufsichtsbehörden** an und muss fortgeführt werden mit der Klärung der Frage, auf **welchen Rechtsgrundlagen** fortgeführte bzw. zukünftige grenzüberschreitende Datenübermittlungen basieren können, um DSGVO-Konformität zu gewährleisten. Im Vereinten Königreich ansässige Unternehmen, die Daten europäischer Bürger verarbeiten, müssen gemäß Art. 27 Abs. 1 DSGVO einen Vertreter in der Union bestellen. **In jedem Fall müssen Unternehmen prüfen, ob sie ihre Datenschutzerklärungen, Einwilligungserklärungen, Betroffenenauskünfte, verbindliche interne Datenschutzvorschriften (sog. Binding Corporate Rules, BCR) sowie Verträge, sonstige Dokumente und technische wie organisatorische Maßnahmen den Gegebenheiten anpassen müssen**. Insbesondere die Anpassung der **Informations- und Hinweispflichten gegenüber Betroffenen** nach Art. 13 Abs. 1 Satz 1 lit. f) und 14 Abs. 1 Satz 1 lit. f) DSGVO sollten keinesfalls vergessen werden. Gibt es keinen baldigen Angemessenheitsbeschluss, so sollten Verantwortliche genau prüfen, ob es **geeignete Garantien** gibt, welche die Datenübermittlung konform mit den EU-Vorgaben ermöglichen. Beispiele hierfür sind entsprechend Art. 46 Abs. 2 DSGVO die EU-Standardvertragsklauseln oder die Binding Corporate Rules oder nach Art. 49 Abs. 1 lit. a) DSGVO die ausdrückliche Einwilligung des Betroffenen, nach lit. b) die Erforderlichkeit zur Vertragserfüllung. Jene Garantien müssen (unter Berücksichtigung der Prüfaspekte des EuGHs im Schrems II Urteil) daraufhin geprüft werden, ob zusätzliche Maßnahmen erforderlich sind, um den Schutz der Daten auf EU-Niveau zu gewährleisten.

Die oben im Kurzüberblick (Management Summary) angegebenen Handlungsempfehlungen können hierbei helfen, die wichtigen Punkte zu adressieren.



Versmold, 15.01.2021
EDV-Unternehmensberatung Floß GmbH
Eva Schlehahn
(Datenschutzberaterin)

3 Annex: DSGVO Normen für Drittland-Datenübermittlungen

KAPITEL V
Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen

Artikel 44
Allgemeine Grundsätze der Datenübermittlung

Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; dies gilt auch für die etwaige Weiterübermittlung personenbezogener Daten durch das betreffende Drittland oder die betreffende internationale Organisation an ein anderes Drittland oder eine andere internationale Organisation. Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.

Artikel 45
Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses

(1) Eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation darf vorgenommen werden, wenn die Kommission beschlossen hat, dass das betreffende Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in diesem Drittland oder die betreffende internationale Organisation ein angemessenes Schutzniveau bietet. Eine solche Datenübermittlung bedarf keiner besonderen Genehmigung.

(2) Bei der Prüfung der Angemessenheit des gebotenen Schutzniveaus berücksichtigt die Kommission insbesondere das Folgende:

a) die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Land bzw. bei der betreffenden internationalen Organisation geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art — auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten — sowie die Anwendung dieser Rechtsvorschriften, Datenschutzvorschriften, Berufsregeln und Sicherheitsvorschriften einschließlich der Vorschriften für die Weiterübermittlung personenbezogener Daten an ein anderes Drittland bzw. eine andere internationale Organisation, die Rechtsprechung sowie wirksame und durchsetzbare Rechte der betroffenen Person und wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen, deren personenbezogene Daten übermittelt werden,

b) die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden in dem betreffenden Drittland oder denen eine internationale Organisation untersteht und die für die Einhaltung und Durchsetzung der Datenschutzvorschriften, einschließlich angemessener Durchsetzungsbefugnisse, für die Unterstützung und Beratung der betroffenen Personen bei der Ausübung ihrer Rechte und für die Zusammenarbeit mit den Aufsichtsbehörden der Mitgliedstaaten zuständig sind, und

c) die von dem betreffenden Drittland bzw. der betreffenden internationalen Organisation eingegangenen internationalen Verpflichtungen oder andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands oder der internationalen Organisation an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben.

(3) Nach der Beurteilung der Angemessenheit des Schutzniveaus kann die Kommission im Wege eines Durchführungsrechtsaktes beschließen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifische Sektoren in einem Drittland oder eine internationale Organisation ein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels bieten. In dem Durchführungsrechtsakt ist ein Mechanismus für eine regelmäßige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen, bei der allen maßgeblichen Entwicklungen in dem Drittland oder bei der internationalen Organisation Rechnung getragen wird. Im Durchführungsrechtsakt werden der territoriale und der sektorale Anwendungsbereich sowie

gegebenenfalls die in Absatz 2 Buchstabe b des vorliegenden Artikels genannte Aufsichtsbehörde bzw. genannten Aufsichtsbehörden angegeben. Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission überwacht fortlaufend die Entwicklungen in Drittländern und bei internationalen Organisationen, die die Wirkungsweise der nach Absatz 3 des vorliegenden Artikels erlassenen Beschlüsse und der nach Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassenen Feststellungen beeinträchtigen könnten.

(5)Die Kommission widerruft, ändert oder setzt die in Absatz 3 des vorliegenden Artikels genannten Beschlusse im Wege von Durchführungsrechtsakten aus, soweit dies nötig ist und ohne rückwirkende Kraft, soweit entsprechende Informationen — insbesondere im Anschluss an die in Absatz 3 des vorliegenden Artikels genannte Überprüfung — dahingehend vorliegen, dass ein Drittland, ein Gebiet oder ein oder mehrere spezifischer Sektor in einem Drittland oder eine internationale Organisation kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels mehr gewährleistet. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen. In hinreichend begründeten Fällen äußerster Dringlichkeit erlässt die Kommission gemäß dem in Artikel 93 Absatz 3 genannten Verfahren sofort geltende Durchführungsrechtsakte.

(6) Die Kommission nimmt Beratungen mit dem betreffenden Drittland bzw. der betreffenden internationalen Organisation auf, um Abhilfe für die Situation zu schaffen, die zu dem gemäß Absatz 5 erlassenen Beschluss geführt hat.

(7) Übermittlungen personenbezogener Daten an das betreffende Drittland, das Gebiet oder einen oder mehrere spezifische Sektoren in diesem Drittland oder an die betreffende internationale Organisation gemäß den Artikeln 46 bis 49 werden durch einen Beschluss nach Absatz 5 des vorliegenden Artikels nicht berührt.

(8) Die Kommission veröffentlicht im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer beziehungsweise Gebiete und spezifischen Sektoren in einem Drittland und aller internationalen Organisationen, für die sie durch Beschluss festgestellt hat, dass sie ein angemessenes Schutzniveau gewährleisten bzw. nicht mehr gewährleisten.

(9) Von der Kommission auf der Grundlage von Artikel 25 Absatz 6 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie durch einen nach dem Prüfverfahren gemäß den Absätzen 3 oder 5 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 46
Datenübermittlung vorbehaltlich geeigneter Garantien

(1) Falls kein Beschluss nach Artikel 45 Absatz 3 vorliegt, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten an ein Drittland oder eine internationale Organisation nur übermitteln, sofern der Verantwortliche oder der Auftragsverarbeiter geeignete Garantien vorgesehen hat und sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.

(2) Die in Absatz 1 genannten geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in

a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,

b) verbindlichen internen Datenschutzvorschriften gemäß Artikel 47,

c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,

d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 genehmigt wurden,

e) genehmigten Verhaltensregeln gemäß Artikel 40 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder

f) einem genehmigten Zertifizierungsmechanismus gemäß Artikel 42 zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.

(3) Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien gemäß Absatz 1 auch insbesondere bestehen in

a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden, oder

b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen.

(4) Die Aufsichtsbehörde wendet das Kohärenzverfahren nach Artikel 63 an, wenn ein Fall gemäß Absatz 3 des vorliegenden Artikels vorliegt.
(5) Von einem Mitgliedstaat oder einer Aufsichtsbehörde auf der Grundlage von Artikel 26 Absatz 2 der Richtlinie 95/46/EG erteilte Genehmigungen bleiben so lange gültig, bis sie erforderlichenfalls von dieser Aufsichtsbehörde geändert, ersetzt oder aufgehoben werden. Von der Kommission auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG erlassene Feststellungen bleiben so lange in Kraft, bis sie erforderlichenfalls mit einem nach Absatz 2 des vorliegenden Artikels erlassenen Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.

Artikel 47
Verbindliche interne Datenschutzvorschriften

(1) Die zuständige Aufsichtsbehörde genehmigt gemäß dem Kohärenzverfahren nach Artikel 63 verbindliche interne Datenschutzvorschriften, sofern diese

a) rechtlich bindend sind, für alle betreffenden Mitglieder der Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gelten und von diesen Mitgliedern durchgesetzt werden, und dies auch für ihre Beschäftigten gilt,

b) den betroffenen Personen ausdrücklich durchsetzbare Rechte in Bezug auf die Verarbeitung ihrer personenbezogenen Daten übertragen und

c) die in Absatz 2 festgelegten Anforderungen erfüllen.

(2) Die verbindlichen internen Datenschutzvorschriften nach Absatz 1 enthalten mindestens folgende Angaben:

a) Struktur und Kontaktdaten der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und jedes ihrer Mitglieder;

b) die betreffenden Datenübermittlungen oder Reihen von Datenübermittlungen einschließlich der betreffenden Arten personenbezogener Daten, Art und Zweck der Datenverarbeitung, Art der betroffenen Personen und das betreffende Drittland beziehungsweise die betreffenden Drittländer;

c) interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften;

d) die Anwendung der allgemeinen Datenschutzgrundsätze, insbesondere Zweckbindung, Datenminimierung, begrenzte Speicherfristen, Datenqualität, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Rechtsgrundlage für die Verarbeitung, Verarbeitung besonderer Kategorien von personenbezogenen Daten, Maßnahmen zur Sicherstellung der Datensicherheit und Anforderungen für die Weiterübermittlung an nicht an diese internen Datenschutzvorschriften gebundene Stellen;

e) die Rechte der betroffenen Personen in Bezug auf die Verarbeitung und die diesen offenstehenden Mittel zur Wahrnehmung dieser Rechte einschließlich des Rechts, nicht einer ausschließlich auf einer automatisierten Verarbeitung

— einschließlich Profiling — beruhenden Entscheidung nach Artikel 22 unterworfen zu werden sowie des in Artikel 79 niedergelegten Rechts auf Beschwerde bei der zuständigen Aufsichtsbehörde beziehungsweise auf Einlegung eines Rechtsbehelfs bei den zuständigen Gerichten der Mitgliedstaaten und im Falle einer Verletzung der verbindlichen internen Datenschutzvorschriften Wiedergutmachung und gegebenenfalls Schadenersatz zu erhalten;

f) die von dem in einem Mitgliedstaat niedergelassenen Verantwortlichen oder Auftragsverarbeiter übernommene Haftung für etwaige Verstöße eines nicht in der Union niedergelassenen betreffenden Mitglieds der Unternehmensgruppe gegen die verbindlichen internen Datenschutzvorschriften; der Verantwortliche oder der Auftragsverarbeiter ist nur dann teilweise oder vollständig von dieser Haftung befreit, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, dem betreffenden Mitglied nicht zur Last gelegt werden kann;

g) die Art und Weise, wie die betroffenen Personen über die Bestimmungen der Artikel 13 und 14 hinaus über die verbindlichen internen Datenschutzvorschriften und insbesondere über die unter den Buchstaben d, e und f dieses Absatzes genannten Aspekte informiert werden;

h) die Aufgaben jedes gemäß Artikel 37 benannten Datenschutzbeauftragten oder jeder anderen Person oder Einrichtung, die mit der Überwachung der Einhaltung der verbindlichen internen Datenschutzvorschriften in der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, sowie mit der Überwachung der Schulungsmaßnahmen und dem Umgang mit Beschwerden befasst ist;

i) die Beschwerdeverfahren;

j) die innerhalb der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, bestehenden Verfahren zur Überprüfung der Einhaltung der verbindlichen internen Datenschutzvorschriften. Derartige Verfahren beinhalten Datenschutzüberprüfungen und Verfahren zur Gewährleistung von Abhilfemaßnahmen zum Schutz der Rechte der betroffenen Person. Die Ergebnisse derartiger Überprüfungen sollten der in Buchstabe h genannten Person oder Einrichtung sowie dem Verwaltungsrat des herrschenden Unternehmens einer Unternehmensgruppe oder der Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, mitgeteilt werden und sollten der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden;

k) die Verfahren für die Meldung und Erfassung von Änderungen der Vorschriften und ihre Meldung an die Aufsichtsbehörde;

l) die Verfahren für die Zusammenarbeit mit der Aufsichtsbehörde, die die Befolgung der Vorschriften durch sämtliche Mitglieder der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, gewährleisten, insbesondere durch Offenlegung der Ergebnisse von Überprüfungen der unter Buchstabe j genannten Maßnahmen gegenüber der Aufsichtsbehörde;

m) die Meldeverfahren zur Unterrichtung der zuständigen Aufsichtsbehörde über jegliche für ein Mitglied der Unternehmensgruppe oder Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem Drittland geltenden rechtlichen Bestimmungen, die sich nachteilig auf die Garantien auswirken könnten, die die verbindlichen internen Datenschutzvorschriften bieten, und

n) geeignete Datenschutzschulungen für Personal mit ständigem oder regelmäßigem Zugang zu personenbezogenen Daten.

(3) Die Kommission kann das Format und die Verfahren für den Informationsaustausch über verbindliche interne Datenschutzvorschriften im Sinne des vorliegenden Artikels zwischen Verantwortlichen, Auftragsverarbeitern und Aufsichtsbehörden festlegen. Diese Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen.

Artikel 48
Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung

Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen unbeschadet anderer Grunde für die Übermittlung gemäß diesem Kapitel jedenfalls nur dann

anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind.

Artikel 49
Ausnahmen für bestimmte Fälle

(1) Falls weder ein Angemessenheitsbeschluss nach Artikel 45 Absatz 3 vorliegt noch geeignete Garantien nach Artikel 46, einschließlich verbindlicher interner Datenschutzvorschriften, bestehen, ist eine Übermittlung oder eine Reihe von Übermittlungen personenbezogener Daten an ein Drittland oder an eine internationale Organisation nur unter einer der folgenden Bedingungen zulässig:

a) die betroffene Person hat in die vorgeschlagene Datenübermittlung ausdrücklich eingewilligt, nachdem sie über die für sie bestehenden möglichen Risiken derartiger Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde,

b) die Übermittlung ist für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich,

c) die Übermittlung ist zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags erforderlich,

d) die Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig,

e) die Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich,

f) die Übermittlung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen erforderlich, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,

g) die Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, aber nur soweit die im Recht der Union oder der Mitgliedstaaten festgelegten Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Falls die Übermittlung nicht auf eine Bestimmung der Artikel 45 oder 46 — einschließlich der verbindlichen internen Datenschutzvorschriften — gestützt werden könnte und keine der Ausnahmen für einen bestimmten Fall gemäß dem ersten Unterabsatz anwendbar ist, darf eine Übermittlung an ein Drittland oder eine internationale Organisation nur dann erfolgen, wenn die Übermittlung nicht wiederholt erfolgt, nur eine begrenzte Zahl von betroffenen Personen betrifft, für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich ist, sofern die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen, und der Verantwortliche alle Umstände der Datenübermittlung beurteilt und auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat. Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis. Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen; dies erfolgt zusätzlich zu den der betroffenen Person nach den Artikeln 13 und 14 mitgeteilten Informationen.

(2) Datenübermittlungen gemäß Absatz 1 Unterabsatz 1 Buchstabe g dürfen nicht die Gesamtheit oder ganze Kategorien der im Register enthaltenen personenbezogenen Daten umfassen. Wenn das Register der Einsichtnahme durch Personen mit berechtigtem Interesse dient, darf die Übermittlung nur auf Anfrage dieser Personen oder nur dann erfolgen, wenn diese Personen die Adressaten der Übermittlung sind.

(3) Absatz 1 Unterabsatz 1 Buchstaben a, b und c und sowie Absatz 1 Unterabsatz 2 gelten nicht für Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchfuhren.

(4) Das öffentliche Interesse im Sinne des Absatzes 1 Unterabsatz 1 Buchstabe d muss im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, anerkannt sein.

(5) Liegt kein Angemessenheitsbeschluss vor, so können im Unionsrecht oder im Recht der Mitgliedstaaten aus wichtigen Gründen des öffentlichen Interesses ausdrücklich Beschränkungen der Übermittlung bestimmter Kategorien von personenbezogenen Daten an Drittländer oder internationale Organisationen vorgesehen werden. Die Mitgliedstaaten teilen der Kommission derartige Bestimmungen mit.

(6) Der Verantwortliche oder der Auftragsverarbeiter erfasst die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Absatzes 1 Unterabsatz 2 des vorliegenden Artikels in der Dokumentation gemäß Artikel 30.