Datenschutzrechtliche Aspekte freiwilliger Kooperation mit Aufsichts- und Ermittlungsbehörden im Rahmen globaler Ermittlungen

In jüngster Zeit häufen sich die Fälle, in denen in- oder ausländische Aufsichts- und Ermittlungsbehörden im Rahmen von aufsichts- oder strafrechtlichen Ermittlungen mit informellen Anfragen an deutsche Unternehmen herantreten und um deren freiwillige Kooperation nachsuchen. Das Ziel dieser Anfragen besteht regelmäßig darin, die betreffenden Unternehmen dazu zu bewegen, ermittlungsrelevante Informationen, darunter Informationen über unternehmensnahe Personen (z.B. über Mitarbeiter, Zulieferer, Kunden etc.), an die Aufsichts- oder Ermittlungsbehörde zu übermitteln. Die Attraktivität eines solchen informellen Vorgehens liegt dabei für Aufsichts- und Ermittlungsbehörden vor allen Dingen in der höheren Geschwindigkeit und Effizienz, da auf diese Weise Verfahrensschritte, die für ein formelles Vorgehen zwingend vorgesehen sind, außer Acht bleiben können.

Angesichts eines solchen Auskunftsersuchens stellt sich für das betreffende Unternehmen die Frage, ob es dem behördlichen Begehren nachkommen soll und darf. Neben wirtschaftlichen Erwägungen wird das Unternehmen dabei zu prüfen haben, ob die in Betracht gezogene Informationsübermittlung überhaupt rechtlich zulässig ist, insbesondere unter dem Blickwinkel des deutschen Datenschutzrechts.[1] Dieses Memorandum stellt den Anwendungsbereich (I.) und die einschlägigen rechtlichen Vorschriften des Bundesdatenschutzgesetzes (BDSG) sowie die in diesem Zusammenhang anzustellenden rechtlichen Erwägungen (II. und III.) überblicksartig dar. Dabei kommt es entscheidend darauf an, ob es sich bei dem potenziellen Empfänger der Informationen um eine deutsche (II.) oder eine ausländische Behörde (III.) handelt. In letzterem Falle ist zudem zwischen der Übermittlung an Behörden in EU- bzw. EWR-Mitgliedstaaten (III.1.) und an Behörden in sog. Drittstaaten (III.2.) zu differenzieren.

I. Die Anwendung des Bundesdatenschutzgesetzes

Das BDSG, das in Teilen die sog. Europäische Datenschutzrichtlinie[2] umsetzt, ist das zentrale Regelwerk für den Umgang mit persönlichen Informationen, konkret: die *Erhebung, Verarbeitung und Nutzung personenbezogener Daten* in Deutschland.[3]

---

1 Andere, teilweise auch strengere rechtliche Vorgaben können an die Stelle des oder zum deutschen Datenschutzrecht hinzutreten, etwa das Telekommunikationsrecht (Telemediengesetz (TMG) und Telekommunikationsgesetz (TKG)) oder, im Falle von Kundendaten von Kreditinstituten, die Grundsätze des Bankgeheimnisses. Sie sind nicht Gegenstand dieses Memorandums.

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. 1995, L 281, S. 31 ff.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG).[4] Im Rahmen aufsichts- oder strafrechtlicher Untersuchungen von Behörden bezüglich des Verhaltens einer oder mehrerer Einzelpersonen, der Mitglieder eines Gesellschaftsorgans oder eines sonstigen Unternehmensgremiums oder sogar des Geschäftsgebarens eines ganzen Unternehmens sind personenbezogene Daten (z.B. Notizbucheinträge, Personalakten, Protokolle, die Dokumentation von Waren-, Dienstleistungs- oder Finanztransaktionen, Informationen über Kunden, Zulieferer und Geschäftspartner) regelmäßig von großer Ermittlungsrelevanz.

Das BDSG regelt die *Erhebung, Verarbeitung und Nutzung* personenbezogener Daten (§ 1 Abs. 2 BDSG).[5] Die ersuchende Empfängerstelle, hier die Aufsichts- oder Ermittlungsbehörde, erhebt die personenbezogenen Daten, denn unter Erhebung ist das Beschaffen von Daten über den Betroffenen zu verstehen (§ 3 Abs. 3 BDSG). Erheblich bedeutender für die Rechtstellung eines von einem behördlichen Auskunftsbegehren betroffenen Unternehmens ist jedoch, dass dieses, entspricht es dem Ersuchen, die entsprechenden Daten verarbeitet. Denn der Begriff der Datenverarbeitung umfasst unter anderem auch das Übermitteln (§ 3 Abs. 4 S. 1 BDSG), das heißt das *Bekanntgeben* gespeicherter oder gewonnener personenbezogener Daten an einen Dritten in einer Weise, dass die Daten an diesen weitergegeben werden (§ 3 Abs. 4 S. 2 Nr. 3 a) BDSG).[6]

II. Die freiwillige Übermittlung personenbezogener Daten an deutsche Aufsichts- und Ermittlungsbehörden

Das BDSG scheint im Hinblick auf die Übermittlung personenbezogener Daten durch nicht-öffentliche an öffentliche Stellen dem Grundgedanken zu folgen, dass dies regelmäßig auf Basis einer *gesetzlichen oder gesetzlich begründeten Übermittlungspflicht* erfolgt. Allerdings lässt § 13 Absatz 1a BDSG erkennen, dass selbst nach der dem BDSG zugrunde liegenden Vorstellung öffentliche Stellen von nicht-öffentlichen Stellen die *freiwillige Übermittlung* personenbezogener Daten erbitten können sollen. Nach dieser Vorschrift hat eine Behörde, die solche Daten

---

[3] In Zukunft wird der Rechtsrahmen für den Schutz personenbezogener Daten in der EU maßgeblich durch die Regelungen der sog. Datenschutz-Grundverordnung bestimmt werden. Der ursprüngliche Kommissionsvorschlag stammt bereits aus dem Jahre 2012 (siehe KOM(2012) 11 endgültig). Für den aktuellen – und wohl finalen – Entwurf, siehe Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 15039/15, 15. Dezember 2015 (nachfolgend „DGVO-Entwurf"). Die Datenschutz-Grundverordnung wird voraussichtlich im Frühjahr 2016 verabschiedet, womit sie Anfang 2018 in Kraft treten könnte (Art. 91 Abs. 2 DGVO-Entwurf).

[4] Vgl. Art. 4 Abs. 1 DGVO-Entwurf.

[5] Vgl. Art. 4 Abs. 3 DGVO-Entwurf.

[6] Vgl. Art. 4 Abs. 3 DGVO-Entwurf („*disclosure by transmission, dissemination or otherwise making available*").

anstelle beim Betroffenen bei einer (anderen) nicht-öffentlichen Stelle erhebt, diese gemäß § 13 Absatz 1a BDSG auf die Vorschrift, wonach diese zur Auskunft verpflichtet ist, andernfalls auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Auch ohne eine gesetzliche oder gesetzlich begründete Übermittlungspflicht bedarf die (freiwillige) Übermittlung von personenbezogenen Daten durch ein betreffendes Unternehmen an eine ersuchende, deutsche Aufsichts- und Ermittlungsbehörde allerdings gemäß § 4 Absatz 1 BDSG grundsätzlich einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen (sog. Verbot mit Erlaubnisvorbehalt).[7]

1. Arbeitnehmerdaten

Das BDSG selbst hält für Datenverarbeitungsvorgänge, insbesondere in den §§ 28 ff. BDSG, eine Reihe von Erlaubnisnormen bereit, welche die Übermittlung personenbezogener Daten unter den darin bestimmten Voraussetzungen erlauben. Dabei enthält § 32 BDSG über die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses zumindest gegenüber § 28 Absatz 1 Satz 1 Nr. 1 BDSG (Durchführung eines Vertragsverhältnisses), nach anderer Ansicht gegenüber allen Erlaubnistatbeständen des § 28 BDSG (Datenerhebung für eigene Geschäftszwecke) die spezielleren Erlaubnistatbestände, soweit es um auf Arbeitnehmer eines Unternehmens bezogene Daten geht, und verdrängen diesen bzw. diese insoweit.[8]

Nach § 32 BDSG dürfen Arbeitnehmerdaten außer für Zwecke des Beschäftigungsverhältnisses nur *zur Aufdeckung von Straftaten* erhoben, verarbeitet oder genutzt werden (§ 32 Abs. 1 S. 2 BDSG). Voraussetzung hierfür ist nach § 32 Absatz 1 Satz 2 BDSG erstens, dass *zu dokumentierende tatsächliche Anhaltspunkte* den Verdacht begründen, dass der Angestellte im Beschäftigungsverhältnis eine Straftat begangen hat. Zweitens muss die Übermittlung der personenbezogenen Daten nach § 32 Absatz 1 Satz 2 BDSG zur

---

[7] Die Einwilligung des Betroffenen ist gemäß § 4a Abs. 1 BDSG nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Auch nach dem DGVO-Entwurf berechtigt eine Einwilligung des Betroffenen grundsätzlich zur Verarbeitung der ihn betreffenden Daten (Art. 6 Abs. 1 a) DGVO-Entwurf). Die Voraussetzungen einer wirksamen Einwilligung sind in Art. 8 DGVO-Entwurf niedergelegt.
Mit Blick auf Arbeitnehmerdaten (dazu I.1.) ist umstritten, ob und inwieweit die Einwilligungen eines betroffenen Arbeitnehmers gegenüber seinem Arbeitgeber überhaupt als auf einer freien Entscheidung beruhend angesehen werden und so für Letzteren eine Befugnis zur Datenverarbeitung begründen kann. Skeptisch hat sich insofern die Artikel 29-Datenschutzgruppe geäußert, siehe Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, WP 48, 13. September 2001, S. 27-28; Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, WP 114, 25. November 2005, S. 13.

[8] Der DGVO-Entwurf enthält eine ausdrückliche Öffnungsklausel, wonach es den Mitgliedstaaten gestattet ist, über die Datenschutz-Grundverordnung hinausgehende Schutzregelungen speziell für die Verarbeitung von Arbeitnehmerdaten zu erlassen (Art. 82 DGVO-Entwurf).

Aufdeckung der Straftat *erforderlich* sein. In dieser Hinsicht ist stets sorgfältig und einzelfallbezogen zu prüfen, ob die mutmaßliche Straftat auch mittels eines Eingriffs von geringerem Gewicht in das verfassungsrechtlich geschützte Recht auf informationelle Selbstbestimmung des Beschäftigten aufgeklärt werden kann. Hier stellt sich die – derzeit noch nicht höchstrichterlich beantwortete – Frage, ob die freiwillige Datenübermittlung (etwa auch in Unkenntnis des Betroffenen) gegenüber einer von der ersuchenden Behörde verbindlich angeordneten Datenübermittlung nicht grundsätzlich einen schwerwiegenderen Eingriff in die Rechtsstellung des Betroffenen darstellt. Drittens muss in jedem Falle ausgeschlossen sein, dass das *schutzwürdige Interesse des Beschäftigten* am Ausschluss der Übermittlung der personenbezogenen Daten nicht überwiegt; diese Interessenabwägung geht nach der gesetzlichen Formulierung jedenfalls dann zugunsten des Beschäftigten aus, wenn Art und Ausmaß der Übermittlung im Hinblick auf den Anlass unverhältnismäßig sind (§ 32 Abs. 1 S. 2 BDSG). In diesem Zusammenhang bedarf es einer umfassenden Verhältnismäßigkeitsprüfung, in welche unter anderem die Eignung der Datenübermittlung zur Aufklärung, ihre Erforderlichkeit im Vergleich mit weniger eingriffsintensiven Mitteln sowie ihre Angemessenheit insbesondere hinsichtlich des Umfangs der Datenübermittlung einzustellen sind. Im Zusammenhang behördlicher Ermittlungen dürfte hier unten anderem auch zu berücksichtigen sein, ob es sich bei dem Betroffenen um einen Unbeteiligten, einen potentiellen Zeugen oder einen mutmaßlichen Täter des untersuchten Fehlverhaltens handelt.[9]

Schließlich sind gemäß § 32 Absatz 3 BDSG etwa bestehende Beteiligungsrechte der Interessenvertretung des Betroffenen, also beispielsweise des Betriebsrats, zu beachten.

2. Sonstige Daten

Soweit § 28 BDSG überhaupt neben § 32 BDSG Anwendung findet, ist auch nach dieser Vorschrift die freiwillige Übermittlung personenbezogener Informationen durch Unternehmen an Aufsichts- und Ermittlungsbehörden nur in engen Grenzen zulässig. Zunächst ist hiernach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten allein *zur Erfüllung eigener Geschäftszwecke* zulässig. Hiernach ist die Datenverarbeitung also schon nur zulässig, wenn sie der eigentlichen Geschäftstätigkeit des betreffenden Unternehmens dient und ein Hilfsmittel hierzu darstellt.

Weiter nennt § 28 Absatz 1 und 2 BDSG eine *Reihe von Erlaubnistatbeständen*, welche die Verarbeitung und Übermittlung personenbezogener Daten unter den darin bestimmten Voraussetzungen erlauben. Danach ist die Übermittlung von Daten unter anderem zulässig, soweit es zur Wahrung berechtigter Interessen des betroffenen Unternehmens oder eines Dritten, zur Abwehr von Gefahren für die

[9] Dabei ist jedoch zu beachten, dass das Bundesdatenschutzgesetz und der Datenschutz freilich auch für (mutmaßliche) Täter von Fehlverhalten gilt.

staatliche oder öffentliche Sicherheit oder zur *Verfolgung von Straftaten* erforderlich ist (§ 28 Abs. 2 Nr. 1 und 2 BDSG).[10] Ob einer oder mehrere dieser Erlaubnistatbestände die freiwillige Übermittlung personenbezogener Daten durch ein Unternehmen an Aufsichts- oder Ermittlungsbehörden rechtfertigt, hängt vom Einzelfall ab.

In jedem Fall muss die Übermittlung zur Verfolgung des jeweiligen Interesses bzw. zur Erfüllung des jeweiligen Zwecks *erforderlich* sein (§ 28 Absatz 1 und 2 BDSG).[11] Dabei ist nach der einschlägigen Literatur ein strenger Beurteilungsmaßstab dergestalt anzusetzen, dass es keine zumutbare Alternative zur begehrten Datenübermittlung geben darf. Ob eine Datenübermittlung auf Basis einer verbindlichen, behördlichen Anordnung als zumutbare Alternative gilt, die einer freiwilligen Datenübermittlung die rechtliche Grundlage entzieht, ist derzeit nicht höchstrichterlich geklärt (vgl. oben II.1.).
Schließlich verlangen alle der genannten Erlaubnistatbestände, dass das *schutzwürdige Interesse des Betroffenen* an dem Ausschluss der Übermittlung nicht überwiegt (so § 28 Abs. 1 S. 1 Nr. 2 BDSG) oder – strenger – dass kein Grund zu der Annahme besteht, dass dieser ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (so § 28 Abs. 2 Nr. 2 BDSG).[12] Unter diesem Gesichtspunkt ist – ähnlich wie im Rahmen des § 32 Absatz 1 Satz 2 BDSG (vgl. oben II.1.) – eine umfassende Interessenabwägung geboten, in deren Rahmen das zugunsten einer Übermittlung streitende Interesse (Eigeninteresse des betreffenden Unternehmens, Drittinteresse der Behörde, staatliches Gefahrenabwehr- bzw. Strafverfolgungsinteresse) gegenüber den Interessen des Betroffenen abzuwägen sind.

III. Die freiwillige Übermittlung personenbezogener Daten an ausländische Aufsichts- und Ermittlungsbehörden

Das BDSG findet Anwendung, wenn die verantwortliche Stelle ihren Sitz in Deutschland hat und dort personenbezogene Daten erhebt oder verarbeitet (§ 1 Abs. 5 BDSG). Diese Voraussetzungen sind erfüllt, wenn das von einem unverbindlichen behördlichen Auskunftsersuchen betroffene Unternehmen seinen Sitz in Deutschland hat und es dort die betreffenden Daten verarbeitet.

---

10 Vgl. Art. 6 Abs. 1 d), e) und f) DGVO-Entwurf.

11 Der Referenzbegriff im DGVO-Entwurf ist „*necessary*“, vgl. Art. 6 Abs. 1 b) bis f) DGVO-Entwurf.

12 Ausdrücklich lediglich in Art. 6 Abs. 1 f) DGVO-Entwurf (Datenverarbeitung im Interesse der verantwortlichen Stelle oder eines Dritten). Allerdings schreibt Art. 6 Abs. 3 DGVO-Entwurf vor, dass die Datenverarbeitung nach Art. 6 Abs. 1 c) und e) DGVO-Entwurf (Datenverarbeitung aufgrund einer Rechtspflicht der verantwortlichen Stelle bzw. im öffentlichen Interesse) auf einer mitgliedstaatlichen oder unionsrechtlichen Rechtsgrundlage beruhen soll, die ihrerseits dem Verhältnismäßigkeitsgrundsatz standzuhalten hat. Hierbei dürften auch die Interessen des Betroffenen zu berücksichtigen sein.

Aus Sicht des betroffenen Unternehmens richtet sich die Zulässigkeit der Übermittlung personenbezogener Daten an ausländische Aufsichts- und Ermittlungsbehörden nach den §§ 4b und 4c BDSG. Diese Vorschriften begründen besondere, über die §§ 28 BDSG ff. hinausgehende Anforderungen für die Übermittlung solcher Daten ins Ausland. Dabei sehen die §§ 4b und 4c BDSG eine Grundunterscheidung zwischen Datentransfers an Stellen innerhalb von EU und EWR (vgl. unten III.1.) und Datentransfers an Stellen außerhalb von EU und EWR (sog. Drittstaaten) (vgl. unten III.2.) vor.

1. Datenübermittlung an Behörden in EU- bzw. EWR-Mitgliedstaaten

Für die Datenübermittlung an Aufsichts- und Ermittlungsbehörden in EU- bzw. EWR-Mitgliedstaaten statuiert § 4b Absatz 1 BDSG, dass die §§ 28 ff. BDSG nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen gelten, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der (ehemaligen) Europäischen Gemeinschaften fallen. Dieses Erfordernis birgt mindestens zwei mögliche Fallstricke für ein Unternehmen, das einem Auskunftsersuchen einer ausländischen Behörde „freiwillig“ nachkommen will.

Erstens bestimmt die Vorschrift, dass die Informationsübermittlung *nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen* erfolgt (§ 4b Abs. 1 BDSG), und impliziert damit, dass sich die grenzüberschreitende Datenübermittlung einschließlich ihrer Voraussetzungen und Grenzen vorrangig nach speziellen Gesetzen oder bi- oder multilateralen Vereinbarungen richtet. Ein solches Gesetz oder eine solche Vereinbarung verdrängt demnach die allgemeinen Datenschutzvorschriften des BDSG einschließlich dessen Übermittlungsvorschriften und legt selbst den rechtlichen Rahmen für eine Übermittlung fest. Hier gilt es genau zu prüfen, ob im vorliegenden Fall eine speziellere Rechtsgrundlage für eine grenzüberschreitende Datenübermittlung besteht und, falls ja, ob deren spezifische Voraussetzungen erfüllt sind. Nur falls dies nicht der Fall ist, kommen die §§ 28 ff. BDSG (vgl. oben II.) zur Anwendung.

Zweitens vermag § 4b Absatz 1 BDSG die Informationsübermittlung zunächst nur insoweit zu rechtfertigen, als sie *Tätigkeiten im Anwendungsbereich des Rechts der (ehemaligen) Europäischen Gemeinschaften* betreffen. Damit ist das Regelwerk der früher sog. ersten Säule der Europäischen Union nach dem Vertrag von Maastricht, das heißt der wirtschaftlichen Zusammenarbeit, in Abgrenzung zur sog. zweiten Säule (Gemeinsame Außen und Sicherheitspolitik) und dritten Säule (Polizeiliche und justizielle Zusammenarbeit in Strafsachen) gemeint. Die Formulierung des § 4b Absatz 1 BDSG orientiert sich an Artikel 3 Absatz 2 der Datenschutzrichtlinie. Danach findet diese auf die Verarbeitung personenbezogener Daten für die Ausübung von Tätigkeiten, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen (darunter ausdrücklich Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die

Tätigkeiten des Staates im strafrechtlichen Bereich), keine Anwendung.[13] Weder aus dem Gesetzeswortlaut geht klar hervor, noch ist höchstrichterlich entschieden, auf wessen Tätigkeit hierbei abzustellen ist – auf die Geschäftstätigkeit des betreffenden Unternehmens (regelmäßig erste Säule) oder die Ermittlungstätigkeit der Aufsichts- und Ermittlungsbehörden (womöglich dritte Säule), an die das Unternehmen die Daten „freiwillig" übermittelt. Vertreter deutscher Datenschutzbehörden haben zu erkennen gegeben, dass sie in diesem Zusammenhang auf die Tätigkeit des betreffenden Unternehmens abstellen wollen – diese dürfte regelmäßig dem Anwendungsbereich des Rechts der (ehemaligen) Europäischen Gemeinschaften unterfallen.[14]

2. Datenübermittlung an Behörden in Drittstaaten, insb. den Vereinigten Staaten

Für die Übermittlung personenbezogener Daten an Aufsichts- oder Ermittlungsbehörden in Drittstaaten wie etwa den Vereinigten Staaten gilt nach § 4b Absatz 2 Satz 1 Alt. 2 BDSG von vornherein ein erhöhter Standard.[15] Danach richtet sich die Übermittlung auch in diesen Fällen *vorrangig nach den hierfür geltenden Gesetzen und Vereinbarungen* (§ 4b Abs. 2 S. 1 Alt. 2 BDSG), darunter Rechtshilfeabkommen wie das zwischen der Bundesrepublik und den Vereinigten Staaten aus dem Jahre 2003 für den Bereich der Strafverfolgung.[16]

Weiter erlaubt § 4b Absatz 2 Satz 1 Alt. 2 BDSG die Informationsübermittlung nur im Hinblick auf *Tätigkeiten im Anwendungsbereich der (ehemaligen) ersten Säule der Europäischen Union*. Auch in diesem Zusammenhang besteht die oben beschriebene Ungewissheit, auf wessen Tätigkeit hierbei abzustellen ist (vgl. oben III.1.).

Ferner ist im Anwendungsbereich des § 4b Absatz 2 Satz 1 Alt. 2 BDSG die Übermittlung grundsätzlich unzulässig, soweit ein *schutzwürdiges Interesse des*

---

13 Auch der DGVO-Entwurf beschränkt seinen materiellen Anwendungsbereichs auf das – freilich viel weiterreichende – Unionsrecht (vgl. Art. 2 Abs. 2 a) DGVO-Entwurf). Allerdings klammert auch er, vergleichbar dem Art. 3 Abs. 2 der Datenschutzrichtlinie, die Datenverarbeitung im Bereich der nationalen Sicherheit und der Strafverfolgung ausdrücklich von seinem Anwendungsbereich aus (Art. 2 Abs. 2 e) DGVO-Entwurf).

14 Für Datentransfers an Aufsichts- und Ermittlungsbehörden in EU- bzw. EWR-Mitgliedstaaten im Rahmen von *Tätigkeiten außerhalb der ersten Säule* gelten dieselben erhöhten Voraussetzungen wie für Datentransfers an in Drittstaaten belegene Stellen (vgl. III.2.).

15 Die Voraussetzungen und Grenzen für die Übermittlung personenbezogener Daten in Drittstaaten sind umfassend in den Art. 40 ff. des DGVO-Entwurfs geregelt.

16 Diesem im BDSG enthaltenen Erfordernis dürfte im DGVO-Entwurf am ehesten dessen Art. 43a entsprechen. Danach darf Urteilen oder Anordnungen drittstaatlicher Gerichte bzw. Behörden, die eine verantwortliche Stelle zur Übermittlung personenbezogener Daten verpflichten, unbeschadet der in den Art. 40 ff. DGVO-Entwurf enthaltenen Erlaubnistatbestände nur Folge geleistet werden, wenn sie auf Grundlage eines zwischen der Europäischen Union oder dem betreffenden Mitgliedsstaat und dem Drittstaat bestehenden völkerrechtlichen Vertrages wie etwa eines Rechtshilfeabkommens beruhen.

Betroffenen an dem Ausschluss der Übermittlung besteht. Nach der gesetzlichen Formulierung liegt ein solches entgegenstehendes, schutzwürdiges Interesse insbesondere vor, wenn bei der Empfängerstelle kein angemessenes Datenschutzniveau gewährleistet ist (§ 4b Abs. 2 S. 1 Alt. 2 Hs. 2 BDSG). In dieser Hinsicht ist die Angemessenheit des Datenschutzniveaus unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen Bedeutung erlangen, allen voran die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen (§ 4b Abs. 3 BDSG).[17] Hierzu hat der Europäische Gerichtshof mit seiner sog. *Safe Harbor*-Entscheidung jüngst hervorgehoben, dass die nationalen Datenschutzbehörden dazu befugt sind, die Angemessenheit des Datenschutzniveaus im Empfängerstaat zu beurteilen.[18] Allerdings sind neben dem Datenschutzniveau auch andere schutzwürdige Interessen des Betroffenen denkbar, die gemäß § 4b Absatz 2 Satz 2 BDSG eine Datenübermittlung ausschließen. Hier könnte der Umstand bedeutsam werden, ob die ersuchende Drittstaatsbehörde zur Erhebung der erbetenen Daten überhaupt befugt ist oder sie sich dadurch sonst rechtswidrig verhält oder – erneut – ob ihr formelle Kanäle zur Erlangung der begehrten Daten zur Verfügung stehen. Ferner dürfte es für die Abwägung von Belang sein, ob es sich bei dem Betroffenen um einen Unbeteiligten, einen potentiellen Zeugen oder einen mutmaßlichen Täter des untersuchten Fehlverhaltens handelt (vgl. oben II.1).[19] Schließlich haben Vertreter deutscher Datenschutzbehörden zu erkennen gegeben, dass sie das Bestehen eines Rechtshilfeabkommens mit dem betreffenden Staat – und damit die für die ersuchende Behörde bestehende Möglichkeit, die begehrten Daten auf förmlichem Wege zu erlangen – als ein relevantes Abwägungskriterium erachten.

Schließlich nennt § 4c BDSG eine Reihe von Ausnahmetatbeständen, die eine Datenübermittlung in einen Drittstaat unter den darin bestimmten Voraussetzungen auch dann gestatten, wenn das dort gewährleistete Datenschutzniveau nicht angemessen im Sinne des § 4b Absatz 2 BDSG ist.[20] Als Grundvoraussetzung verlangt § 4c Absatz 1 BDSG wiederum, dass es sich um *Tätigkeiten* handelt, die ganz oder teilweise in den *Anwendungsbereich des Rechts der (ehemaligen) Europäischen Gemeinschaften* fallen – mit der diesem Erfordernis eigenen rechtlichen Ungewissheit (vgl. oben III.1). Im Übrigen gestatten die in § 4c Absatz 1 BDSG enumerativ aufgeführten Ausnahmetatbestände eine Informationsübermittlung in Drittstaaten nur in engen Grenzen. Dies ist – neben

---

17 Zur Datenübermittlung auf Grundlage einer Angemessenheitsentscheidung der Kommission (und die bei deren Erlass zu berücksichtigenden Kriterien), siehe Art. 41 DGVO-Entwurf.

18 EuGH, Entscheidung vom 6. Oktober 2015 (*Schrems*) – C-362/14).

19 Insbesondere bei Unbeteiligten könnte das Interesse, nicht in die „Mühlen" der drittstaatlichen Justiz zu geraten, einen abwägungsrelevanten Belang darstellen.

20 Zu den Voraussetzungen und Grenzen einer Datenübermittlung ohne eine Angemessenheitsentscheidung der Kommission, siehe Art. 44 DGVO-Entwurf.

dem Tatbestand der Einwilligung[21] – etwa der Fall, wenn die Übermittlung für die *Wahrung eines wichtigen öffentlichen Interesses* oder zur *Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht* erforderlich ist (§ 4c Abs. 1 Nr. 4 BDSG).[22] Dabei darf es sich nach Verlautbarungen der Artikel 29-Datenschutzgruppe bei dem wichtigen öffentlichen Interesse nicht lediglich um ein unilaterales Interesse der ersuchenden Behörde handeln.[23] In diesem Zusammenhang stellt sich unter anderem die Frage, ob „bloßes Verwaltungsunrecht" ein hinreichend wichtiges öffentliches Interesse im Sinne des § 4c Absatz 1 Nr. 4 BDSG darstellt. Ferner haben Vertreter deutscher Datenschutzbehörden hinsichtlich der Geltendmachung von Rechtsansprüchen zu erkennen gegeben, dass diese auch tatsächlich vor Gericht erfolgen muss, wohingegen eine Geltendmachung in verwaltungs- und anderen behördlichen Verfahren nicht genügt.[24] In jedem dieser Fälle muss der Datentransfer nach § 4c Absatz 1 Nr. 4 BDSG zur Verfolgung des jeweiligen Zwecks *erforderlich* sein.[25] Insofern gilt auch im Anwendungsbereich des § 4c Absatz 1 BDSG, dass eine Übermittlung auf dieser Grundlage nur dann gerechtfertigt ist, wenn dem Auskunftsverlangen der ausländischen Behörden nicht auf weniger eingriffsintensive Art und Weise Rechnung getragen werden kann.

Schließlich ermöglicht § 4c Absatz 2 BDSG die Übermittlung personenbezogener Daten an in Drittstaaten belegene Stellen mit behördlicher Genehmigung. Danach kann die zuständige Datenschutzbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an Stellen in Drittstaaten genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist (§ 4c Abs. 2 Hs. 1 BDSG). Die Inanspruchnahme dieses Erlaubnistatbestands setzt voraus, dass das betreffende Unternehmen von der ersuchenden Drittstaatsbehörde entsprechende Garantien einfordert und erhält und

---

21 Vgl. § 4c Abs. 1 Nr. 1 BDSG. Siehe zu den Voraussetzungen einer wirksamen Einwilligung Fn. 7.

22 Vgl. Art. 44 Abs. 1 d) DGVO-Entwurf („*important reasons of public interest*") und Art. 44 Abs. 1 e) DGVO-Entwurf („*establishment, exercise or defence of legal claims*").

23 Artikel 29-Datenschutzgruppe, Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24.10.1995, WP 114, 25. November 2005, S. 17; *dies.*, Stellungnahme 6/2002 zur Übermittlung von Informationen aus Passagierlisten und anderen Daten von Fluggesellschaften an die Vereinigten Staaten, WP 66, 24. Oktober 2002, S. 7. Diesbezüglich stellt der DGVO-Entwurf klar, dass das relevante öffentliche Interesse *im Unionsrecht oder im Recht des Mitgliedstaats, dem die verantwortliche Stelle unterliegt, anerkannt* sein muss (Art. 44 Abs. 5 DGVO-Entwurf).

24 Der Zusatz *vor Gericht*, wie er in der deutschen Fassung der Datenschutzrichtlinie (dort Art. 26 Abs. 1 d)) und dem BDSG (dort § 4c Abs. 1 Nr. 4) zu finden ist, ist in der englischen Fassung der Datenschutzrichtlinie nicht enthalten. Auch im DGVO-Entwurf findet er sich nicht (siehe Fn. 22). Damit dürfte dieser Ausnahmetatbestand zukünftig auch in Deutschland die Datenübermittlung zum Zwecke des Geltendmachens von Ansprüchen oder der Rechtsverteidigung in behördlichen (Ermittlungs-)Verfahren ermöglichen.

25 Referenzbegriff im DGVO-Entwurf ist hier wieder „*necessary*", vgl. Art. 44 Abs. 1 b) bis f) DGVO-Entwurf.

es sich hinsichtlich einer Genehmigung mit der zuständigen Datenschutzbehörde ins Benehmen setzt.

IV. Ausblick

Die Einhaltung der Vorgaben des deutschen Datenschutzrechts dürfte für deutsche Unternehmen, die von einem informellen Auskunftsersuchen insbesondere von Drittstaatsbehörden (z.B. aus den Vereinigten Staaten) betroffen waren, in der Vergangenheit häufig einen untergeordneten Stellenwert gehabt haben – zu gering sind die potentiell zu erwartenden Sanktionen in Deutschland und zu abschreckend die potentiell zu erwartenden Sanktionen im Drittstaat. Mit dem Inkrafttreten der sog. Datenschutz-Grundverordnung, deren Verabschiedung für das Frühjahr 2016 zu erwarten ist, dürfte sich dies ändern. Denn nach dem aktuellen – und wohl finalen – Entwurf der Datenschutz-Grundverordnung dürfen die zuständigen Datenschutzbehörden im Falle von Verstößen zukünftig Geldbußen in Höhe von bis zu 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes eines Unternehmens verhängen.[26]

* * *

Sie können dieses Memorandum gerne innerhalb Ihrer Institution weiterleiten. Für Fragen zu den Themen dieses Memorandums stehen Dr. Thomas Kopp (tkopp@cgsh.com) und Dr. Valentin Pfisterer (vpfisterer@cgsh.com) aus dem Frankfurter Büro von Cleary Gottlieb sowie unsere Partner und Counsel, die auf unserer Website http://www.clearygottlieb.com/de unter Praxisbereiche - Regionen – Deutschland – Anwältinnen und Anwälte aufgeführt sind, gerne zur Verfügung.

[26] Art. 79 Abs. 3a DGVO-Entwurf.

Büros

NEW YORK
One Liberty Plaza
New York, NY 10006-1470, USA
T: +1 212 225 2000
F: +1 212 225 3999

WASHINGTON
2000 Pennsylvania Avenue, NW
Washington, DC 20006-1801, USA
T: +1 202 974 1500
F: +1 202 974 1999

PARIS
12, rue de Tilsitt
75008 Paris, Frankreich
T: +33 1 40 74 68 00
F: +33 1 40 74 68 88

BRÜSSEL
Rue de la Loi 57
1040 Brüssel, Belgien
T: +32 2 287 2000
F: +32 2 231 1661

LONDON
City Place House
55 Basinghall Street
London EC2V 5EH, England
T: +44 20 7614 2200
F: +44 20 7600 1698

MOSKAU
Cleary Gottlieb Steen & Hamilton LLC
Paveletskaya Square 2/3
Moscau, Russland 115054
T: +7 495 660 8500
F: +7 495 660 8505

FRANKFURT
Main Tower
Neue Mainzer Strasse 52
60311 Frankfurt am Main
T: +49 69 97103 0
F: +49 69 97103 199

KÖLN
Theodor-Heuss-Ring 9
50688 Köln
T: +49 221 80040 0
F: +49 221 80040 199

ROM
Piazza di Spagna 15
00187 Rom, Italien
T: +39 06 69 52 21
F: +39 06 69 20 06 65

MAILAND
Via San Paolo 7
20121 Mailand, Italien
T: +39 02 72 60 81
F: +39 02 86 98 44 40

HONGKONG
Cleary Gottlieb Steen & Hamilton (Hong Kong)
Hysan Place, 37th Floor
500 Hennessy Road, Causeway Bay
Hong Kong
T: +852 2521 4122
F: +852 2845 9026

PEKING
Cleary Gottlieb Steen & Hamilton LLP
45th Floor, Fortune Financial Center
5 Dong San Huan Zhong Lu
Chaoyang District
Beijing 100020, China
T: +86 10 5920 1000
F: +86 10 5879 3902

BUENOS AIRES
CGSH International Legal Services, LLP-Sucursal Argentina
Avda. Quintana 529, 4to piso
1129 Ciudad Autonoma de Buenos Aires
Argentina
T: +54 11 5556 8900
F: +54 11 5556 8999

SÃO PAULO
Cleary Gottlieb Steen & Hamilton
Consultores em Direito Estrangeiro
Rua Funchal, 418, 13 Andar
São Paulo, SP Brazil 04551-060
T: +55 11 2196 7200
F: +55 11 2196 7299

ABU DHABI
Al Sila Tower, 27th Floor
Abu Dhabi Global Market Square
Al Maryah Island, PO Box 29920
Abu Dhabi, United Arab Emirates
T: +971 2 412 1700
F: +971 2 412 1899

SEOUL
Cleary Gottlieb Steen & Hamilton LLP
Foreign Legal Consultant Office
19F, Ferrum Tower
19, Eulji-ro 5-gil, Jung-gu
Seoul 100-210, Korea
T:+82 2 6353 8000
F:+82 2 6353 8099