23850

ZD
ZEITSCHRIFT FÜR
DATENSCHUTZ

RALF DEUTLMOSER / ALEXANDER FILIP

Europäischer Datenschutz und US-amerikanische (e-)Discovery-Pflichten

Ein Praxisleitfaden für Unternehmen

European Data Privacy versus U.S. (e-)Discovery Obligations

A Practical Guide For Enterprises

www.zd-beck.de

ZD-Beilage
6/2012

2. Jahrgang 1. Juni 2012
Verlag C.H.Beck München

O830201206

Inhaltsverzeichnis

ZEITSCHRIFT FÜR DATENSCHUTZ
ZD
BEILAGE

RALF DEUTLMOSER / ALEXANDER FILIP

Europäischer Datenschutz und US-amerikanische (e-)Discovery-Pflichten

Ein Praxisleitfaden für Unternehmen

Datenverwendungskette
Transkontinentale Rechtsstreitigkeiten
Export personenbezogener Daten
Transparenz
Anonymisierung
Fernmeldegeheimnis

■ Der Konflikt zwischen U.S.-amerikanischen prozessualen Offenlegungspflichten im Rahmen der (e-)Discovery und deutschem bzw. europäischem Datenschutzrecht ist derzeit kaum beherrschbar. Trifft die Aussage der Sedona Konferenz aus dem Dezember 2011 zu, wonach das Thema so komplex und verwirrend ist, dass es weitgehend ignoriert wird, gehen die betroffenen Unternehmen ein ganz erhebliches Risiko ein. Die Strafen sind empfindlich und die möglichen Folgen in den amerikanischen Zivilverfahren reichen bis hin zum sofortigen Unterliegen im Prozess.
Diese Sonderbeilage zeigt einen Weg auf, den Konflikt praktisch handhabbar zu machen und berücksichtigt dabei die Veröffentlichungen der Art. 29-Datenschutzgruppe, der Sedona Konferenz und den Entwurf der EU-Datenschutz-Verordnung (DS-GVO) aus dem Januar 2012.
Es wird aufgezeigt, dass jede Verwendung personenbezogener Daten der gesonderten Erlaubnis bedarf. Der Schutz berechtigter Interessen der verantwortlichen Stelle kann auf der allgemeinen datenschutzrechtlichen Prüfungsebene, die Erforderlichkeit der Verwendung in Bezug auf Rechtsansprüche vor einem ausländischen Gericht auf der exportspezifischen Prüfungsebene zu einer solchen Erlaubnis führen. Neben der „normalen" Interessenabwägung ist jedoch eine exportspezifische Abwägung durchzuführen, hinsichtlich derer die Waagschale zunächst zu Ungunsten des Exports geneigt ist. Im Regelfall ist der Export nur zulässig, nachdem alle zumutbaren Filterungen durchgeführt wurden, nach der Anonymisierung oder Pseudonymisierung und nach ordnungsgemäßer Unterrichtung der Betroffenen.
Abschließend wird das Telekommunikationsrecht am Arbeitsplatz betrachtet. Sofern der Arbeitgeber den Privatgebrauch von Internet oder E-Mail-System explizit erlaubt oder duldet, ist er als Diensteanbieter anzusehen. Die Telekommunikationsdaten unterliegen dann dem besonderen Schutz des Fernmeldegeheimnisses. Dieser endet mit dem Abschluss der Datenübertragung, der dann eintritt, wenn der Telekommunikationsteilnehmer die ausschließliche Kontrolle über die Daten erlangt.

■ The conflict between European Data Privacy laws and U.S. (e-) discovery obligations is currently almost unmanageable for German and European enterprises. Provided that the Sedona Conference was correct in its December 2011 statement, whereby the subject is „an area often thought of as so complex and confounding that it has been largely ignored", the relevant enterprises run a tremendous risk. The penalties are severe and a directed verdict in the US litigation could be the ultimate consequence of non-compliance.
This guide for enterprises will provide a practically usable and comprehensive approach to manage the respective conflict. It takes into account the publications of the Article 29 Working Party, of the Sedona Conference, and the January 2012 draft EU regulation.
It will be demonstrated that each and every handling of personal data requires a specific permission. Safeguarding the data controller's legitimate interests can provide such permission on a general level and the necessity with respect to foreign legal claims on the export-specific level. Besides the general balancing test, an export-specific additional balancing test has to be performed, with respect to which the scale initially tips on the side of non-transfer. Generally, the export is legitimate only after all reasonable culling, anonymization or pseudonymization, and information of the data subjects is done.
Finally, telecommunication privacy at the workplace is examined. Provided that the employer explicitly allows for or tolerates private use of the Internet or e-mail services, it has to be considered a provider of telecommunication services. As a consequence, the telecommunication information is protected by the right to telecommunication privacy until the conclusion of the data transmission. This conclusion occurs only once the participant gains exclusive control over the data.

■ Die Originalfassung dieser Publikation (vgl. hierzu im 2. Teil der Beilage) wurde in englischer Sprache erstellt. Besonderer Dank gebührt für das Entwerfen der Übersetzung und wertvollen Input Rechtsreferendar Olaf Preuss, München.

I. Der Unternehmer – „Diener zweier Herren"

Europäische Unternehmer und Unternehmen, die in Rechtsstreitigkeiten in den USA verwickelt sind, versuchen stets, zwei Herren zu dienen:[1] dem europäischen Datenschutzrecht und dem US-amerikanischen Zivilprozessrecht, insbesondere den (e-)Discovery Verpflichtungen. Es überrascht nicht, dass dieser Versuch erhebliche Schwierigkeiten aufwirft, insofern „[...] Konflikte zwischen dem Datenschutzrecht einerseits und anderen Grundrechten sowie anderen rechtlichen Anforderungen (z.B. e-Discovery [...]) andererseits auftreten, welche die Unternehmen in die Zwangslage bringen, nicht mehr zu wissen, welches Recht sie befolgen sollen".[2]

Beiderseits des Atlantiks erkennt man das resultierende Dilemma sowie den potenziellen Schaden für den Welthandel: Während anerkannt ist, dass grenzüberschreitende Datenflüsse für die Ausweitung des internationalen Handels notwendig sind,[3] wird die Komplexität der Regeln über den internationalen Transfer persönlicher Daten als beträchtliche Behinderung der Geschäftstätigkeiten der Wirtschaftsakteure wahrgenommen.[4] Das Dilemma hat ein solches Ausmaß angenommen, dass die *American Bar Association* im Februar 2012 die Auffassung vertrat, die gegenwärtige Entscheidungspraxis der US-amerikanischen Gerichte, „die als engstirnig oder die Interessen und Gebräuche anderer Rechtsordnungen nur unzulänglich berücksichtigend angesehen werden könne, könnte das Wachstum des Welthandels hemmen".[5]

Das Problem wird zusätzlich durch unterschiedliche Umsetzungen und Auslegungen der aktuellen EU-Datenschutz-Richtlinie (DS-RL) durch die nationalen Gesetzgeber und relevanten Aufsichtsbehörden der EU-Mitgliedstaaten verschärft – was schon bei solchen Grundprinzipien wie der Definition der personenbezogenen Daten beginnt.[6] Sollte auf europäischer Ebene der Schritt von der gegenwärtigen DS-RL zu einer zukünftigen Verordnung vollzogen werden, wie aktuell vorgeschlagen, würden solche Unterschiede zwischen den Mitgliedstaaten erheblich reduziert.

Die maßgeblichen Problemkreise erfordern nicht nur eine Klarstellung der europäischen und einzelstaatlichen Gesetze,[7] sondern eher einen bahnbrechend neuen Ansatz – einen „New Deal" – insofern der aktuelle Rechtsrahmen der EU dem Megatrend der globalen Datentransfers vorausgeht.[8] Es bleibt abzuwarten, ob die Konsultation zur Zukunft des Rechtsrahmens für den Datenschutz, welche die *EU-Kommission* im Juli 2009 anlaufen ließ und die wahrscheinlich zu einer europäischen Datenschutz-Grundverordnung (DS-GVO) führen wird, einen präzisen und handhabbaren Rechtsrahmen liefern wird. Das ist besonders deshalb kritisch, weil die Strafdrohungen und verwaltungsrechtlichen Sanktionen, welche der gegenwärtige Entwurf vorsieht, gewaltig sind und sich auf bis zu 2% des weltweiten Jahresumsatzes der verantwortlichen Stelle belaufen.[9] Leider deutet im aktuellen Entwurf nichts auf einen „New Deal" hin. Trotz der Erklärung, dass die Rechtssicherheit gestärkt werden solle,[10] bleibt der Entwurf – zumindest im Hinblick auf die in dieser Veröffentlichung diskutierten Kernfragen – weit von einer „kopernikanischen Wende" entfernt.[11] Im gegenwärtigen Stadium scheint es so, als ob eine der größten Herausforderungen, denen sich eine zukünftige Verordnung zu stellen hat, das Thema des Datentransfers in Drittstaaten,[12] ungenügend in Angriff genommen wird.

Trotz der praktischen Bedeutung dieser Frage für Unternehmen und sogar die Weltwirtschaft sehen sich die Parteien eines Rechtsstreits bedauerlicherweise erheblichen Unsicherheiten ausgesetzt,[13] und es ist schwierig, im Hinblick auf die Auswirkungen des Datenschutzrechts auf (e-)Discovery Anforderungen präzise Empfehlungen zu geben.[14] Schlimmer noch, gemäß der *Sedona Conference* (*TSC*) wird dieses Rechtsgebiet häufig als derart komplex und verwirrend erachtet, dass es weitgehend ignoriert worden sei.[15] Fasst man diesen Befund zusammen, so sind alle Beteiligten unzufrieden mit den gegenwärtigen Regelungen.[16]

Seit biblischen Zeiten gilt, dass niemand „zwei Herren dienen [kann]: Entweder er wird den einen hassen und den andern lieben, oder er wird an dem einen hängen und den andern verachten".[17] Eingedenk dieser Weisheit bietet diese Veröffentlichung eine praktische Anleitung an, die Unternehmen zum angemessenen Umgang mit den gegebenen Risiken befähigt, die mit den beschriebenen Kernfragen verbunden sind, und ihnen dabei hilft, die Wahl zwischen „Gott und Mammon"[18] oder zumindest zwischen dem EU-Datenschutzrecht und den US-amerikanischen (e-)Discovery Verpflichtungen zu vermeiden. Diese Veröffentlichung stellt einen zweisprachigen Leitfaden zu diesem Thema zur Verfügung, der auf beiden Seiten des Atlantiks eingesetzt werden kann, und es damit Parteien, Behörden und Gerichten ermöglicht, die „gebotene Achtung gegenüber dem Datenschutzrecht ausländischer Staaten an den Tag" zu legen, wie es Principle 1 der TSC International Principles on Discovery, Disclosure and Data Protection (TSC International Principles) verlangt.[19]

Leider gibt es keine Patentrezepte, aber nach einer Darstellung des Hintergrunds (vgl. unter II.), führt die Analyse der Anforderungen an den Umgang mit personenbezogenen Daten zu Zwecken transkontinentaler Prozessführung im Allgemeinen (vgl. unter III.) zu einem Leitfaden, anhand dessen ein Normfall abgehandelt werden kann. Letztlich ist eine einzelfallbezogene Anpassung erforderlich; zumindest wird aber die Grundlage für eine generelle strategische Herangehensweise im Hinblick auf jeden einzelnen Schritt in der Datenverwendungskette geschaffen, welche sowohl in den USA als auch in Deutschland gut vertretbar ist (vgl. unter IV. bis VII.). Am Ende wird eine Reihe von Fragen bzgl. des TK-Rechts am Arbeitsplatz und der daraus resultierenden Handlungseinschränkungen für Arbeitgeber behandelt, soweit diese eine private Nutzung des Internet am Arbeitsplatz erlauben oder tolerieren (vgl. unter VIII.).

---

1 *Carlo Goldoni*, „Arlecchino servitore di due padroni", 1745.
2 *ICC*, Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data, December 2009, S. 3.
3 DS-GVO, Erwägungsgrund 78.
4 Memorandum(2012), S. 4.
5 *American Bar Association*, „Section of International Law, Resolution 103, Report to the House of Delegates", S. 2.
6 S.a. *American Chamber of Commerce to the European Union*, „Response to the Commission Consultation on Protection of Personal Data", S. 4 f.
7 *Spies/Schröder*, MMR 2008, 275, 281.
8 *American Chamber of Commerce to the European Union,* „Response to the Commission Consultation on Protection of Personal Data", S. 2.
9 DS-GVO, Art. 78, 79. Aus Gründen der besseren Lesbarkeit wird hier und im Folgenden einheitlich der Begriff der „verantwortlichen Stelle", den der deutsche Gesetzgeber im BDSG in Umsetzung der RL 95/46/EG festgelegt hat, auch im Kontext der Ausführungen zur DS-GVO verwendet, obwohl der europäische Gesetzgeber eine geringfügig abweichende Terminologie einführt. Die DS-GVO spricht von „den für die Datenverarbeitung Verantwortlichen".
10 DS-GVO, Erwägungsgrund 6.
11 *Kuner*, 11 PVLR 06, 14.
12 *Kuner*, 11 PVLR 06, 9.
13 *Spies*, MMR 7/2007, S. V, VI.
14 *Hoppe/Braun*, MMR 2010, 80, 84.
15 *TSC*, „International Principles on Discovery, Disclosure & Data Protection", 2011, S. VI.
16 *Kuner*, 11 PVLR 06, 9.
17 *Matthäus*, 6, 24.
18 *Matthäus*, 6, 24.
19 *TSC*, „International Principles on Discovery, Disclosure & Data Protection", 2011, S. 7.

Das Ergebnis der Analyse kann in einem Satz zusammengefasst werden: Das Gebot der Stunde lautet: „Abwägen".

II. Hintergrund und Leitbilder

US-amerikanische Discovery-Pflichten und EU-Datenschutz sowie andere Rechte stehen zweifellos im Widerstreit zueinander. Der Konflikt kann jedoch nur dann richtig begriffen und Wege, um die Differenzen zu überwinden, können nur dann entwickelt werden, wenn man die grundlegenden Unterschiede in der Prozesskultur sowie die unterschiedlichen Datenschutzkonzepte berücksichtigt. Vor einer detaillierten Analyse sind daher der Hintergrund des Konflikts sowie die datenschutzrechtlichen Leitbilder zu untersuchen.

1. Das Konzept der „pre-trial discovery"

Die Hauptursache für den Konflikt, der in dieser Veröffentlichung diskutiert wird, liegt im US-amerikanischen Konzept der elektronischen und konventionellen „pre-trial discovery" („Discovery"). Im Großen und Ganzen lässt sich Discovery – so wie sie z.B. in den US Federal Rules of Civil Procedure angelegt ist – als das formelle Verfahren verstehen, nach welchem die Parteien eines Rechtsstreits und Drittbeteiligte Informationen, die für den Rechtsstreit von Belang sind, zur Verfügung stellen müssen und ihrerseits von den übrigen Beteiligten erlangen können. Zu den Hauptzwecken der Discovery gehört es, so viele (möglicherweise) streiterhebliche Tatsachen wie möglich aufzudecken, faire Voraussetzungen in Bezug auf ein etwaiges Informationsungleichgewicht für den Rechtsstreit zu schaffen und es den Prozessparteien ganz allgemein zu ermöglichen, die Fakten und Beweisantritte eines Streits besser zu verstehen.[20]

Um eine umfassende Discovery zu gewährleisten, existiert in den USA eine entsprechende Verpflichtung, Informationen, die für den Rechtsstreit relevant werden können, aufzubewahren, sobald der Rechtsstreit begonnen hat oder vernünftigerweise mit ihm zu rechnen ist.[21] Solche Informationen sind zu sichern und dürfen weder innerhalb noch außerhalb eines ordentlichen Dokumentenmanagementprozesses vernichtet werden. In der Praxis versenden Prozessparteien in den USA sog. „litigation hold letters" an potenzielle Verwahrer und Träger relevanter Informationen (im Weiteren „custodians" oder „Informationsträger" genannt). Diese Briefe setzen die Informationsträger im Detail von anhängigen oder vernünftigerweise zu erwartenden Gerichtsverfahren in Kenntnis und weisen sie an, die beschriebenen Informationen zu sichern.

So seltsam es aus europäischer Perspektive auch erscheinen mag, selbst – und gerade – solche Informationen sind umfasst, die der Partei schaden, die die Last der Sicherung und Offenlegung trägt: die sprichwörtliche „smoking gun" ist dem Gegner auszuhändigen. Aus US-amerikanischer Sicht ist diese Verpflichtung zur Sicherung und Offenlegung ein Grundpfeiler der Prozessführung und ein wesentliches Element der Rechtspflege.

Wegen der Bedeutung, die der Discovery zukommt, sollte eine gemeinsame Verständigung zwischen den Parteien schon in einem frühen Stadium des Rechtsstreits erzielt werden. Um dieses Ziel zu fördern, verlangt Rule 26f der US Federal Rules of Civil Procedure von den Prozessparteien, dass sie sich frühzeitig im Verfahren treffen und beraten, um die relevanten Themen zu erörtern und Vereinbarungen zu schließen.

Die meisten Länder des kontinentaleuropäischen Rechtskreises, die dem „Civil Law"-System folgen, wählen einen gegensätzlichen Ansatz. Demnach obliegt es prinzipiell jeder Prozesspartei, die Tatsachen beizubringen, die für sie günstig sind, und den entsprechenden Beweis zu führen. Sofern eine Partei auf Beweismittel zurückgreifen möchte, die sich in den Händen der anderen Partei befinden, hat sie die gesuchten Beweismittel zunächst allgemein zu bezeichnen.[22] „Civil-Law"-Systeme unterstützen im Großen und Ganzen keine „fishing expeditions",[23] also Verfahren, die allein der Ausforschung des Gegners dienen; pre-trial Discovery stellt in diesen Rechtsordnungen kein bekanntes Konzept dar, und zivilprozessuale Offenlegungspflichten sind kaum vorhanden.

Parteien, die in den USA prozessieren, stehen daher – anders als in Europa – unter hohem Druck, (elektronische oder konventionelle) Dokumente und Materialien, die möglicherweise relevant für einen Rechtsstreit sind, zu identifizieren und zu übergeben. Solche Dokumente werden in fast allen Fällen personenbezogene Daten von Angestellten, Zulieferern, Kunden oder anderen Dritten enthalten. Wenn diese personenbezogenen Daten vom europäischen Datenschutzrecht – genau genommen, zumindest derzeit, von der nationalen Umsetzung in das Recht der Mitgliedstaaten – umfasst sind, können Konflikte zwischen den Sicherungs- und Offenlegungspflichten einerseits und dem jeweiligen Datenschutzrecht andererseits entstehen.

2. Datenschutz – ein Grundrecht

Nicht nur die Unterschiede im Zivilprozessrecht sind für den Zusammenprall der Rechtskulturen verantwortlich, sondern auch das Gewicht, welches dem Datenschutz im Allgemeinen beigemessen wird. 1983 urteilte das *BVerfG*, dass Art. 2 Abs. 1 Grundgesetz (GG) i.V.m. Art. 1 Abs. 1 GG ein Grundrecht auf informationelle Selbstbestimmung enthält. Das Recht umfasst die Garantie, dass jeder Einzelne über die Offenlegung und den Gebrauch seiner personenbezogenen Daten selbst entscheiden kann. In dieses Grundrecht darf nur eingegriffen werden, wenn der Eingriff durch ein überragendes öffentliches Interesse gerechtfertigt ist und auf der Grundlage eines formellen Gesetzes erfolgt.[24] Neben dem genannten Grundrecht des deutschen GG bieten Art. 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) und Art. 16 Abs. 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ähnliche Rechte. Es ist jedoch zu beachten, dass Datenschutz kein absolutes Recht ist, wie der *EuGH* betont.[25]

Ohne tiefer in die Materie einzusteigen, kann festgehalten werden, dass der Missbrauch der Regierungsgewalt durch das nationalsozialistische Regime und seine Verbündeten vor dem und während des Zweiten Weltkriegs einerseits und durch das kommunistische Regime besonders in der Zeit des Kalten Krieges andererseits einen der Hauptgründe für die große Bedeutung darstellt, welche dem Datenschutz in Europa beigemessen wird. Massive Datensammlungsbestrebungen durch die öffentliche Gewalt, selbst wenn diese aus Gründen der nationalen Sicherheit erfolgen, treffen heutzutage nicht selten auf heftige Kritik.[26] Die historischen Hintergründe sowie die gegenwärtigen politischen Diskussionen und Entwicklungen sind stets zu bedenken, wenn man die Unterschiede zwischen dem europäischen und dem US-amerikanischen Ansatz zum Datenschutz beurteilt und das jeweilige Recht kommentiert.

---

20 *TSC*, „International Principles on Discovery, Disclosure & Data Protection", 2011, S. 1.

21 *TSC*, „International Principles on Discovery, Disclosure & Data Protection", 2011, S. 2.

22 Ausweislich von § 142 Abs. 1 Satz 1 ZPO kann ein Gericht die Vorlage der von einer Partei in Bezug genommenen Urkunden und sonstigen Unterlagen anordnen. § 142 ZPO erlaubt jedoch keine Ausforschung oder „fishing expeditions", da ein spezifisches Dokument zumindest identifizierbar sein muss. Die bloße Behauptung, dass derartige Dokumente normalerweise in der Sphäre des Gegners oder eines Dritten vorhanden sind, reicht nicht aus; *Musielak*, ZPO, 8. Aufl. 2011, § 142 Rdnr. 4.

23 *Art. 29-Datenschutzgruppe*, WP 158, S. 4; *Hanloser*, DuD 2008, 785.

24 BVerfGE 65, 1, 43.

25 Memorandum(2012), S. 6 m.w.Nw.

26 *Künast*, ZRP 2008, 201, 203.

Der Austausch mit und das Verständnis der jeweils anderen Rechtskultur werden durch die Tatsache erschwert, dass nicht einmal die Fachausdrücke übereinstimmend gebraucht werden. In dieser Veröffentlichung wird daher zwischen Datenschutz („data privacy") und Datensicherheit („data protection") i.S.d. technischen Schutzes der Daten unterschieden.

3. Rechtsgrundlagen des europäischen und deutschen Datenschutzrechts

Auf europäischer Ebene stellt die RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (die DS-RL) den gegenwärtig maßgeblichen Gesetzesakt dar.[27] Das Bundesdatenschutzgesetz (BDSG) setzt nicht nur die DS-RL um, sondern implementiert auch die Leitprinzipien, die das *BVerfG*, wie oben diskutiert, aufgestellt hat.[28]

Konsultationen, die die *EU-Kommission* im Juli 2009 initiierte, führten zu dem „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 – DS-GVO)", welcher offiziell am 25.1.2012 verkündet wurde. Abgesehen von der DS-GVO umfasst der Vorschlag ein erklärendes Memorandum bzgl. der vorgeschlagenen Verordnung („Memorandum(2012)") und einen Richtlinienvorschlag „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr". Wegen des übermäßig langen und komplexen EU-Gesetzgebungsprozesses und einer vorgeschlagenen zweijährigen Übergangszeit wird eine Verordnung wahrscheinlich nicht vor 2015, 2016 oder sogar 2017 in Kraft treten.[29] Relevante Artikel der DS-GVO werden in dieser Veröffentlichung diskutiert, wenn sie Einsichten in das gegenwärtige Verständnis des Rechts auf europäischer Ebene vermitteln oder einen Ausblick auf das bieten, was von einer künftigen Verordnung zu erwarten steht.

Es bleibt abzuwarten, ob der am Ende des Verfahrens stehende Rechtsakt eine „Kopernikanische Wende" in Gang setzt, welche den Fokus weg von „papierbasierten, bürokratischen Anforderungen" und hin zu „praktischer Compliance, Harmonisierung und Übertragung von Verantwortung auf den Einzelnen" lenkt.[30] Wenigstens im Hinblick auf die hier diskutierten Kernpunkte erscheint dies als unwahrscheinlich. In Hinblick auf die DS-GVO wurde bereits in der Literatur ausgeführt, dass darin der Bedarf an einem präzisen und gleichzeitig praxistauglichen Regelwerk offensichtlich bisweilen aus dem Auge verloren wurde.[31]

4. Personenbezogene Daten

Das BDSG befasst sich nur mit „personenbezogenen Daten". In Übereinstimmung mit der Intention des europäischen Gesetzgebers[32] definiert § 3 Abs. 1 BDSG den Begriff als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener).

Personenbezogene Daten erfassen alle Angaben über persönliche oder sachliche Verhältnisse. Dies schließt objektive oder subjektive Aussagen gleich welcher Art über eine Person ein, unabhängig von der Stellung oder Eigenschaft der Person. Dabei ist gleichgültig, in welchem Format (alphabetisch, numerisch, grafisch, fotografisch oder akustisch) und in welcher Form (papiergebunden, computergespeichert, auf Audio-/Videoband aufgezeichnet) die Daten vorliegen.[33] Eine ausdrückliche oder implizite Aussage über die Teilnahme an einem Treffen oder die Aufzeichnung einer gemachten Aussage reichen insoweit aus. Die meisten E-Mails erfüllen das Kriterium, insofern sie z.B. die E-Mail-Adressen von Absender und Empfänger, die Stellung des Absenders im Unternehmen und eine Aussage des Absenders (den Inhalt der E-Mail) enthalten.[34]

Die Einzelangabe muss sich auf ein bestimmtes oder bestimmbares Individuum beziehen. Dies ist der Fall, wenn sie über das Individuum oder über Tatsachen, die sich auf das Individuum beziehen, Auskunft gibt.[35] Oder genauer gesagt, wenn sie auf die Identität, kennzeichnende Merkmale oder das Verhalten eines Individuums Bezug nimmt oder wenn eine solche Information verwendet wird, um die Art und Weise, wie mit der Person umgegangen wird oder wie sie eingeschätzt wird, festzulegen oder zu beeinflussen.[36]

Im Hinblick auf Informationen von Unternehmen können Unternehmensangehörige, Angehörige von Zulieferern oder Kunden sowie jede andere natürliche dritte Person betroffen sein.

Da der Begriff der personenbezogenen Daten nicht nur private, sondern auch berufliche Angelegenheiten erfasst, enthalten auch die meisten Unternehmens-E-Mails personenbezogene Daten.[37] Mit anderen Worten: praktisch jede einzelne Unternehmens-E-Mail fällt nach europäischem und nationalem Recht unter den Begriff der personenbezogenen Daten.[38]

5. Besondere Arten personenbezogener Daten

Eine Untergruppe der personenbezogenen Daten wird als so sensibel erachtet, dass die DS-RL und das deutsche Umsetzungsgesetz hierfür spezielle Schutzvorkehrungen vorsehen. Die sensiblen „besonderen Arten personenbezogener Daten" umfassen ausdrückliche oder sich aus dem Kontext ergebende Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben (§ 3 Abs. 9 BDSG).[39] Im Umgang mit besonderen Arten personenbezogener Daten ist besondere Sorgfalt angebracht. Die nötigen Schutzvorkehrungen werden im betreffenden Kapitel ausgeführt.

6. Räumlicher Anwendungsbereich des BDSG

Das BDSG findet Anwendung, wenn personenbezogene Daten in Deutschland erhoben, verarbeitet oder genutzt werden. Die Verarbeitung findet in Deutschland statt, wenn der physische Verarbeitungsvorgang in Deutschland durchgeführt wird, ins-

27 Official Journal L 281, 23/11/1995, 0031 – 0050.
28 S. unter II.2.
29 Es bestehen erhebliche Zweifel daran, ob die DS-GVO mit dem GG vereinbar ist. Eine detaillierte Auseinandersetzung mit dieser Frage kann in dieser Veröffentlichung nicht erfolgen.
30 *Kuner*, 11 PVLR 06, 1.
31 *Kuner*, 11 PVLR 06, 14.
32 *Art. 29-Datenschutzgruppe*, WP 136, S. 4.
33 *Art. 29-Datenschutzgruppe*, WP 136, S. 6 f.
34 Die *Art. 29-Datenschutzgruppe* legt dar, dass etwa das Rezept eines Arztes an einen anonymen Patienten persönliche Angaben über die verordnende Person enthält, WP 136, S. 7.
35 Däubler/*Weichert*, BDSG Kompaktkommentar, 3. Aufl., § 3 Rdnr. 19.
36 *Art. 29-Datenschutzgruppe*, WP 136, S. 9; *Art. 29-Datenschutzgruppe*, WP 105, S. 8; die *Art. 29-Datenschutzgruppe* führt aus, drei Elemente könnten alternativ verwendet werden, um festzustellen, ob solche Verbindungen bestehen: Inhalt (Informationen über Personen werden preisgegeben), Zweck (Informationen werden verwendet, um Personen auf eine bestimmte Art und Weise zu behandeln), oder Ergebnis (die Informationen haben wahrscheinlich eine Auswirkung auf die Rechte und Interessen einer Person); *Art. 29-Datenschutzgruppe*, WP 136, S. 10 f.
37 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, S. 181 f.
38 *FIOS*, Webcast v. 21.4.2009, E-Mails in den USA sind personenbezogene Daten in der EU und anderswo; *TSC*, Framework for Analysis of Cross-Border Discovery Conflicts, S. 9.
39 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 3 Rdnr. 65.

besondere wenn sich der Server oder Computer in Deutschland befindet.[40] Im Hinblick auf die Erhebung und Nutzung personenbezogener Daten reicht es aus, wenn die Daten sich in Deutschland befinden oder die verantwortliche Stelle in Deutschland tätig ist.[41]

Die DS-GVO wird den räumlichen Anwendungsbereich aus praktischer Sicht nicht einschränken. Art. 3 Abs. 1 DS-GVO besagt, dass sie Anwendung findet für die Datenverarbeitung im Zusammenhang mit den Aktivitäten der Niederlassung einer verantwortlichen Stelle in der Europäischen Union.

7. Normadressaten des BDSG

Während die DS-RL hinsichtlich der zu erreichenden Ziele nur für die Mitgliedstaaten verbindlich ist und gem. Art. 288 Abs. 3 AEUV den innerstaatlichen Stellen die Wahl der Form und der Mittel bei der Umsetzung überlässt, richtet sich das BDSG als deutsches Umsetzungsgesetz nicht nur an die staatlichen Behörden,[42] sondern auch an Rechtsträger des Zivilrechts, sofern nicht die Daten ausschließlich für persönliche oder nicht-gewerbliche Zwecke erhoben oder verarbeitet werden.[43]

8. Zulässige Datenverwendung

§ 4 Abs. 1 BDSG bringt den wichtigsten Grundsatz des deutschen Datenschutzrechts zum Ausdruck. Danach ist jede Erhebung, Verarbeitung und Nutzung personenbezogener Daten (zusammenfassend „Umgang mit personenbezogenen Daten" oder auch im Folgenden kurz „Datenverwendung") nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlauben oder der Betroffene eingewilligt hat. In den Grenzen seines weiten Anwendungsbereichs postuliert das BDSG somit ein gesetzliches Verbot mit Erlaubnisvorbehalt.[44]

Jeder Schritt und jede Zwecksetzung in einer gegebenen Datenverwendungskette, in diesem Fall der Abfolge von Handlungen im Zivilrechtsstreit, ist einzeln zu beurteilen. Falls sich der Zweck der Datenverwendung ändert, muss die Rechtmäßigkeit neu beurteilt werden im Hinblick auf den neuen Zweck. Mit anderen Worten, rechtmäßiges Handeln zu einem bestimmten Zweck impliziert nicht die Rechtmäßigkeit in Bezug auf einen neuen oder weitergehenden Zweck.

In diesem Zusammenhang bedeutet Erheben von Daten (§ 3 Abs. 3 BDSG) die Datenbeschaffung, während unter den Begriff des Verarbeitens gem. § 3 Abs. 4 BDSG u.a. die folgenden Vorgänge fallen:

- Speichern: Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger;
- Verändern: inhaltliches Umgestalten gespeicherter personenbezogener Daten;
- Übermitteln: Bekanntgeben personenbezogener Daten an einen Dritten, sei es durch Weitergabe an den Dritten, sei es durch Einsichtnahme oder Abruf der Daten durch den Dritten.

Nur am Rande sei erwähnt, dass das französische Verbotsgesetz („blocking statute") das Auskunftsersuchen, die Nachforschung oder Offenlegung in Schrift, Wort oder anderer Form von Dokumenten oder Informationen wirtschaftlicher, kommerzieller, industrieller, finanzieller oder technischer Natur zu Beweiszwecken im Rahmen ausländischer gerichtlicher oder behördlicher Verfahren verbietet.[45]

9. Datenvermeidung und Datensparsamkeit

Die Grundsätze der Datenvermeidung und Datensparsamkeit stellen gem. § 3a Satz 1 BDSG weitere Eckpfeiler des deutschen und europäischen Datenschutzrechts dar. Sie ergeben sich aus dem Recht auf informationelle Selbstbestimmung und besagen im Wesentlichen,[46] dass so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen sind. Wann immer mehrere gleich effektive Mittel zur Erfüllung einer Aufgabe vorhanden sind, ist stets das mildeste Mittel zu wählen, bei welchem die erforderliche Datenverwendung das geringste Ausmaß hat.[47]

Art. 5 lit. c) DS-GVO gibt in Bezug auf die Verarbeitung personenbezogener Daten vor, dass personenbezogene Daten „dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Mindestmaß beschränkt sein" müssen.

Aus der Zweckgebundenheit der Erlaubnis und ihrer Beschränkung auf das erforderliche Mindestmaß folgt, dass Daten zu anonymisieren oder pseudonymisieren sind, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert (§ 3a Satz 2 BDSG). Darüber hinaus sind die Daten, sobald der Verwendungszweck erreicht ist, zu löschen.[48] Der Vorgang der Löschung stellt also, mit anderen Worten, das Ende jeder Datenverwendungskette dar und ist schon in ihrer Grundstruktur zu verankern.

Die DS-GVO vertritt das Konzept der Datenvermeidung sogar noch ausdrücklicher als die DS-RL.[49] Danach sollen nicht unverhältnismäßig viele Daten erfasst werden und die Speicherfrist auf das „unbedingt erforderliche Mindestmaß" beschränkt sein.[50]

Aus den Grundsätzen des § 3a Satz 1 BDSG folgt als weitere Konsequenz, dass der Bestand personenbezogener Daten ständig überprüft und im Umfang so weit reduziert werden muss, wie es durch Maßnahmen möglich ist, die vernünftigerweise gefordert werden können.

Die Verwendung personenbezogener Daten zu Prozesszwecken kann nur dann gerechtfertigt sein, wenn diese für den konkreten Rechtsstreit relevant sind. Die Relevanz wird jedoch in der US-amerikanischen Rechtsordnung anders definiert als im deutschen Recht. Nach dem US-amerikanischen Ansatz reicht es zur Begründung von Sicherungs- und Offenlegungspflichten bereits aus, dass die betreffenden Daten möglicherweise zu prozessrelevanten Beweistatsachen führen können. Dagegen versteht das europäische Datenschutzrecht das Kriterium eher i.S.v. „direkter und objektiver Relevanz". Die Entscheidung für eines der beiden Konzepte sollte nicht abstrakt, sondern im Kontext jedes einzelnen Schritts in der Datenverwendungskette getroffen werden.

III. Verwendung personenbezogener Daten für transkontinentale Rechtsstreitigkeiten – Prinzipien und Grundregeln

Nach der Darstellung des allgemeinen Hintergrunds richtet sich das Augenmerk nun auf die Besonderheiten des Umgangs mit personenbezogenen Daten im Kontext transkontinentaler Rechtsstreitigkeiten. In diesem Kapitel werden Leitlinien und Prinzipien definiert, ehe anschließend die Ergebnisse auf jeden

40 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, S. 176 f.
41 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, S. 177 f.
42 Däubler/*Weichert*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 1 Rdnr. 9.
43 Sofern die Privatperson die Daten zur Nutzung in Datenverarbeitungsanlagen erhebt, solche Systeme zur Verwendung nutzt oder Daten in oder aus nicht automatisierten Dateien erhebt oder solche Systeme für die Verwendung nutzt, spricht man von Datenerhebung und -verwendung.
44 Däubler/*Weichert*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4 Rdnr. 9.
45 *TSC*, Framework for Analysis of Cross-Border Discovery Conflicts, S. 21.
46 BVerfGE 65, 1, 43.
47 *Conrad*, CR 2005, 537.
48 *Brisch/Laue*, RDV 2010, 1, 3; *Spies/Schröder*, MMR 2008, 275, 278.
49 *Kunert*, 11 PVLR 06, 5.
50 DS-GVO, Erwägungsgrund 30.

Schritt der Datenverwendungskette praktisch angewendet werden.

Dieses Kapitel wird das Folgende zeigen: Da aus tatsächlichen und rechtlichen Gründen so gut wie nie eine wirksame Einwilligung aller Betroffenen vorliegen wird,[51] erfordert der Umgang mit personenbezogenen Daten für Zwecke transkontinentaler Rechtsstreitigkeiten eine Beurteilung in zwei Stufen: Allgemeine Datenverwendungsvoraussetzungen müssen ebenso erfüllt sein wie exportspezifische zusätzliche Anforderungen. Im Allgemeinen dürfen personenbezogene Daten zur Wahrung eines berechtigten Interesses der verantwortlichen Stelle verwendet werden, in diesem Fall zur Verteidigung gegen einen Rechtsanspruch, sofern die Abwägung ergibt, dass die Verwendung verhältnismäßig ist.[52] Der Export der Daten erfordert zusätzlich, dass eine spezifische, dem Datenexport Rechnung tragende Interessenabwägung bestanden ist. Diese Interessenabwägung, bei der sich in der Ausgangslage die Waagschale zu Ungunsten des Exports neigt, ist unabhängig davon notwendig, ob die Grundsätze des „sicheren Hafens", ein Übermittlungsvertrag, oder die „Notwendigkeit in Bezug auf Rechtsansprüche" die Rechtsgrundlage für den Export bilden.[53] Unternehmen sind zudem gut beraten, die Datenschutzbeauftragten so früh wie möglich einzubeziehen, die Betroffenen in angemessenem Umfang zu unterrichten, und dem Risiko angemessene Datensicherheitsmaßnahmen zu etablieren.

1. Die Datenverwendungskette in transkontinentalen Rechtsstreitigkeiten

Es wurde bereits erwähnt, dass der Umgang mit personenbezogenen Daten auf jeder Stufe der Datenverwendungskette einer Erlaubnis bedarf, die in Gestalt einer Einwilligung oder durch Rechtsvorschrift gegeben sein kann (vgl. hierzu unter II.8.). Der Einfachheit halber sei insoweit das folgende vierstufige Schema verwendet:

- Zuerst sind die Informationen, die möglicherweise personenbezogene Daten enthalten, zu identifizieren und sicher zu speichern. Es muss dabei sichergestellt werden, dass jeder ordentliche oder außerordentliche Löschungsvorgang angehalten wird („Sicherung").
- Sobald die Sicherung vollzogen ist, werden die Daten intern überprüft und genutzt („interne Datenverwendung"), ehe:
- externe Anwälte und Experten die Informationen durchsehen („externe Datenverwendung").
- In einem letzten Schritt sind die Informationen der gegnerischen Prozesspartei oder dem US-amerikanischen Gericht auszuhändigen („Offenlegung"). Die Übermittlung von personenbezogenen Daten in einen Drittstaat („Export") findet vor oder während der externen Datenverwendung, spätestens aber zum Zeitpunkt der Offenlegung statt.

2. Einwilligung: wohl kaum eine praktikable Option

Die Einwilligung des Betroffenen wäre die vorzugswürdige und – im Prinzip – einfachste Form, die Zulässigkeit des Umgangs mit personenbezogenen Daten herbeizuführen. Leider erscheint es für die meisten Fälle als unwahrscheinlich, dass eine wirksame Einwilligung im Zusammenhang mit Rechtsstreitigkeiten und Gerichtsprozessen in den USA erreicht werden kann.[54] Im Einklang mit diesem Befund zog schon 2005 die *Art. 29-Datenschutzgruppe*[55] den Schluss: „Das Erfordernis der Einwilligung kann also als vermeintlich gute Lösung erscheinen, die auf den ersten Blick einfach, in der Praxis jedoch komplex und schwerfällig ist"[56]. Diese negative Einschätzung beruht sowohl auf tatsächlichen als auch auf rechtlichen Gründen.

In praktischer Hinsicht sind die allgemeinen Voraussetzungen für eine wirksame Einwilligung der Betroffenen – insbesondere in Fällen, wo sich die Sicherung und Datenverwendung auf Hunderttausende oder Millionen von Dokumenten oder Dateien erstreckt – fast unmöglich zu erfüllen. Gem. § 4a Abs. 1 BDSG setzt die Wirksamkeit der Einwilligung voraus, dass jeder einzelne Betroffene vorab in angemessener Weise über den vorgesehenen Zweck der Sicherung oder einer späteren Verwendung der Daten unterrichtet worden ist. Eine solche Unterrichtung erfordert nicht nur, dass Umfang und Zweck der Sicherung der Daten mitgeteilt werden, sondern überdies, dass, zumindest in späteren Stadien, die potenziellen Empfänger der personenbezogenen Daten angegeben werden.[57] Eine Blankovollmacht, z.B. im Arbeitsvertrag oder in einer eigenständigen Erklärung, die von allen Beschäftigten unterschrieben wird, welche die Datenverwendung zu allen möglichen Zwecken legitimieren würde, stellt keine wirksame Einwilligung dar.[58]

Wenn es gegenwärtig auch theoretisch möglich scheint, eine spezifische Klausel in den Individualarbeitsvertrag aufzunehmen, die die Datenverwendung zu zivilprozessualen Zwecken abdeckt, so ist doch anzunehmen, dass derzeit in der Praxis eine solche Klausel in den meisten Arbeitsverträgen fehlt. Zudem dürfte es sehr schwierig sein, eine Klausel so präzise zu fassen, dass der Betroffene durch sie eine wirksame Einwilligung in die Datenverwendung zu Prozesszwecken im Voraus erklärt. Natürlich kann auf diesem Wege auch nicht die Einwilligung von nicht im Unternehmen beschäftigten Betroffenen wie Zulieferern, Kunden oder sonstigen Dritten erlangt werden.

Ebenso wenig kann eine Einwilligung im Wege von Kollektivvereinbarungen, wie z.B. Betriebsvereinbarungen, erteilt werden.[59] Im Ergebnis muss die Einwilligung individuell und in Bezug auf den tatsächlichen Zweck – Rechtsstreitigkeiten im Ausland – erteilt werden. Daher stellt mit Blick auf Rechtsstreitigkeiten, die eine große Menge von personenbezogenen Daten berühren, die Einholung der Einwilligung der Betroffenen keinen praktikablen Lösungsweg dar. Zudem ist festzuhalten, dass die Einwilligung jederzeit, ohne Angabe von Gründen und ohne nachteilige Folgen für den Beschäftigten, frei widerruflich ist.

Sollten besondere Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG betroffen sein, so muss sich die Einwilligung ausdrücklich auf diese Daten beziehen. Es wird vertreten, dass dabei die besonderen Arten personenbezogener Daten in den Wortlaut der Einwilligung aufzunehmen sind.[60]

Die Einwilligung muss schriftlich erfolgen (eine einfache E-Mail erfüllt diese Anforderung nicht), sofern nicht wegen besonderer Umstände eine andere Form angemessen ist.[61] Die Einwilligung muss vor der Datenverwendung erfolgen, eine nachträgliche Genehmigung heilt den Gesetzesverstoß nicht.[62]

Der wichtigste rechtliche Grund dafür, dass eine wirksame Einwilligung kaum möglich ist, besteht darin, dass diese auf einer freien Entscheidung des Betroffenen beruhen muss. Er muss da-

51 S. unter III.2.
52 S. unter III.4.
53 S. unter III.5.
54 *Spies*, MMR 7/2007, S. V, VII.
55 Die *Art. 29-Datenschutzgruppe* wurde auf Basis von Art. 29 der RL 95/46/EG errichtet. Es handelt sich bei ihr um ein unabhängiges Beratungsgremium auf europäischer Ebene in Hinblick auf Datenschutz und Datensicherheit. Ihre Aufgaben sind in Art. 30 der RL 95/46/EG sowie Art. 15 der RL 2002/58/EC beschrieben.
56 *Art. 29-Datenschutzgruppe*, WP 114, S. 11.
57 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4b Rdnr. 8.
58 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, S. 79; *Art. 29-Datenschutzgruppe*, WP 114, S. 12.
59 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4a Rdnr. 3; *Pröpper/Römermann*, MMR 2008, 514, 515 f.
60 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4a Rdnr. 42 m.w.Nw.
61 § 4a Abs. 1 Satz 2 BDSG.
62 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4b Rdnr. 4.

für eine tatsächliche Chance erhalten, seine Einwilligung zu versagen oder zu widerrufen, ohne dass er wegen seiner Entscheidung negative Konsequenzen zu befürchten hätte.[63] Für den Fall, dass es sich bei dem Betroffenen um einen Beschäftigten der verantwortlichen Stelle handelt, empfiehlt es sich, ausdrücklich zu erklären, dass der Beschäftigte keine nachteiligen Auswirkungen erleiden wird, wenn er nicht einwilligt oder die erteilte Einwilligung zu einem späteren Zeitpunkt widerruft.[64]

Es sei darauf hingewiesen, dass nach Ansicht einiger Autoren ein Arbeitnehmer auf Grund der Natur des Arbeitsverhältnisses (fast) nie wirksam einwilligen kann;[65] überzeugender ist jedoch die Auffassung, dass eine widerlegbare Vermutung gegen die Freiwilligkeit besteht.[66] Von einem praktischen Blickwinkel aus betrachtet begibt sich die verantwortliche Stelle zumindest auf schwankenden Boden, wenn sie sich auf die Einwilligung eines Beschäftigten verlässt. Daher ist vom Gebrauch der Einwilligung abzuraten, solange es einen anderen Weg gibt.

Die DS-GVO verschärft die Anforderungen sogar dahingehend, dass sie eine Einwilligung nur dann als wirksam anerkennt, wenn sie „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage" explizit erfolgt.[67] Die Einwilligung soll dann unter Zwang erfolgen, wenn der Betroffene keine „echte Wahlfreiheit hat und somit nicht in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden."[68] Außerdem stellt die Einwilligung nach Art. 7 Nr. 4 DS-GVO keine Rechtsgrundlage dar, „wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht". Als Musterbeispiel für solch ein erhebliches Ungleichgewicht nennt Erwägungsgrund Nr. 34 der DS-GVO das Arbeitsverhältnis. Damit wird in Zukunft die Einwilligung als Rechtsgrundlage für die Verwendung arbeitnehmerbezogener Daten nicht nur „schwieriger",[69] sondern praktisch gar nicht mehr heranziehbar sein.

Auch wenn es unmöglich sein mag, eine wirksame Einwilligung von allen Betroffenen zu erlangen, so könnte es dennoch sinnvoll sein, sich soweit um Einwilligungen zu bemühen, wie es praktisch und rechtlich möglich ist. Jeder Umgang mit personenbezogenen Daten, der von einer wirksamen Einwilligung gedeckt ist, verringert den Umfang an personenbezogenen Daten, für deren Verwendung eine andere Form der Erlaubnis erforderlich ist. Da die Menge der Informationen eine Rolle spielt im Hinblick auf die Abwägung der jeweiligen Interessen, könnte daraus ein positiver Einfluss auf die Gesamtbeurteilung folgen. Es scheint, dass in Übereinstimmung damit in der Praxis einige Beklagte wenigstens von denjenigen Betroffenen, die „litigation hold letters" erhalten, die Einwilligung einzuholen versuchen.

3. Der zweistufige Ansatz: Allgemeine Anforderungen und spezifische Export-Anforderungen

Die Beurteilung der Verwendung „deutscher" personenbezogener Daten für Zwecke eines US-amerikanischen Prozesses erfordert eine zweistufige Herangehensweise. Zunächst müssen die allgemeinen Anforderungen erfüllt sein, insofern jeder einzelne Schritt in der Datenverwendungskette eine spezifische Erlaubnis erfordert. Zusätzlich müssen dann die weitergehenden besonderen Anforderungen erfüllt sein, welche die §§ 4b und 4c BDSG für die Übermittlung personenbezogener Daten ins Ausland aufstellen. Im Wesentlichen wird auf einer ersten Ebene beurteilt, ob die Datenverwendung zulässig wäre, wenn es sich um einen rein inner-europäischen Rechtsstreit handelte. Auf der zweiten Ebene ist zu beurteilen, ob der Export der personenbezogenen Daten in Einklang mit dem deutschen und europäischen Datenschutzrecht steht.

Die *Art. 29-Datenschutzgruppe* hat 2009 in dem Arbeitspapier „über Offenlegungspflichten i.R.d. vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery)" für jeden Schritt bei der Datenverwendung Lösungen vorgeschlagen. Das Arbeitspapier beruht auf der Grundannahme, dass die zivilprozessualen Anforderungen einer ausländischen Rechtsordnung mit den datenschutzrechtlichen Anforderungen der DS-RL in Einklang gebracht werden müssen.[70] Dabei stellt das Arbeitspapier ausdrücklich fest, dass „die Richtlinie Übermittlungen für Verfahrenszwecke nicht ausschließt", aber auch, dass „bestimmte Datenschutzerfordernisse [...] erfüllt sein" müssen, und schlägt entsprechende Leitlinien vor.[71] Danach soll der Konflikt „zwischenstaatlich – etwa durch Einführung weiterer globaler Konventionen – geregelt werden".[72] Auch wenn die *Art. 29-Datenschutzgruppe* natürlich keinerlei Gesetzgebungskompetenz hat, steht zu erwarten, dass ihre Empfehlungen auf diesem hochgradig unbeständigen Rechtsgebiet von den maßgeblichen europäischen und nationalen Behörden sorgfältig ausgewertet und beachtet werden.[73]

4. Allgemeine Datenverwendungsvoraussetzung: Schutz berechtigter Interessen der verantwortlichen Stelle

Der erste Teil des zweistufigen Ansatzes verlangt, dass die allgemeinen Datenverwendungsvoraussetzungen des § 28 BDSG erfüllt werden.[74] Dabei wird die Verwendung personenbezogener Daten zum Zwecke transkontinentaler Rechtsverfolgung eher auf die Verfolgung eigener Geschäftszwecke als durch eine Einwilligung gestützt werden können. Gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist die Datenverwendung zulässig „[...] als Mittel für die Erfüllung eigener Geschäftszwecke [...] soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und [soweit] kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt [...]."

Es ist zu beachten, dass § 32 BDSG, der die Verwendung personenbezogener Daten für Zwecke eines Beschäftigungsverhältnisses regelt, grundsätzlich nicht anwendbar ist auf Datenverwendungen im Zusammenhang mit allgemeinen geschäftsbezogenen Rechtsstreitigkeiten von Unternehmen. Nach dem Willen des Gesetzgebers erlaubt § 32 Abs. 1 BDSG die Datenverwendung, soweit es erforderlich ist, für die Einstellungsentscheidung oder für die Durchführung, Beendigung und Abwicklung des Arbeitsverhältnisses.[75] Daher bleibt § 28 Abs. 1 Satz 1 Nr. 2 BDSG anwendbar, wenn die Verwendung der personenbezogenen Daten nicht dem Beschäftigungsverhältnis als solchem, sondern anderen eigenen Interessen der verantwortlichen Stelle dient, wie z.B. der Durchführung eines allgemeinen Rechtsstreits des Unternehmens.

---

63 Die Gesetzesbegründung, die namentlich Beschäftigungsverhältnisse diskutiert, führt aus, dass in Fällen, in denen Druck ausgeübt werden kann, die Einwilligung ohne Zwang erteilt werden muss, in: *Simitis/Dammann/Geiger*, Dokumentation zum Bundesdatenschutzgesetz, S. 108.

64 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4b Rdnr. 9.

65 Gem. dem *Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit* (*HmbBfDI*) dürften Beschäftigte allgemein nicht die notwendige Unabhängigkeit besitzen, um wirksam einwilligen zu können, 22. TB, S. 95; 18. TB, S. 197.

66 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4b Rdnr. 23 bezugnehmend auf die Leitsätze des *BGH* DB 2008, 2188, 2189 = MMR 2008, 731 m. Anm. *Grapentin*.

67 DS-GVO, Art. 4 Abs. 8.

68 DS-GVO, Erwägungsgrund 33.

69 *Kunert*, 11 PVLR 06, 6.

70 *Art. 29-Datenschutzgruppe*, WP 158, S. 2.

71 *Art. 29-Datenschutzgruppe*, WP 158, S. 7.

72 *Art. 29-Datenschutzgruppe*, WP 158, S. 2.

73 *TSC*, International Overview 2009 – Deutschland, S. 103.

74 Die Besonderheiten bzgl. der Verwendung besonderer Arten personenbezogener Daten werden in Kapitel III.8 behandelt.

75 Empfehlungen des *Innenausschusses des Deutschen Bundestages*, BT-DS 16/13657, S. 20 f.

a) Berechtigtes Interesse

Die Anwendung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG setzt das Vorliegen eines berechtigten Interesses der verantwortlichen Stelle voraus.[76] Jedes rechtliche, wirtschaftliche oder sogar ideelle Interesse reicht in dieser Hinsicht aus.[77] Die Verteidigung gegen eine Klage, die sich gegen die verantwortliche Stelle richtet, begründet ein berechtigtes Interesse in diesem Sinne, auch wenn die Klage im Ausland erhoben wurde.[78] Der Gerechtigkeit wäre wenig gedient, wenn die Möglichkeiten der verantwortlichen Stelle, ihre Rechte durchzusetzen oder zu verteidigen, unnötig beschränkt würden. Diese Auffassung wird auch dadurch gestützt, dass § 28 Abs. 6 Nr. 3 BDSG sogar die Verwendung besonderer Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) für zulässig erklärt, soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und schutzwürdige Interessen des Betroffenen am Unterbleiben der Datenverwendung nicht überwiegen.

Die Datenverwendung ist notwendig, wenn das berechtigte Interesse nicht, jedenfalls nicht in zumutbarer Weise, anders wahrgenommen werden kann.[79] Nach *Brisch/Laue* wird vom Gesetz insoweit ein strenges Erforderlichkeitsgebot aufgestellt.[80] Indessen ist offensichtlich, dass eine effektive Rechtsverteidigung vor einem ausländischen Gericht die Befolgung der lex fori verlangt.

b) Verhältnismäßigkeit: Abwägung der Interessen

Es reicht jedoch nicht aus, dass ein berechtigtes Interesse der verantwortlichen Stelle existiert, um jegliche Verwendung personenbezogener Daten zu rechtfertigen. Ein dogmatischer Hinweis auf weitere Einschränkungen findet sich darin, dass nur die Datenverwendung erlaubt ist, die „erforderlich ist zur Wahrung" des jeweiligen Interesses. Darüber hinaus verlangt § 28 Abs. 1 Satz 1 Nr. 2 BDSG, dass „[...] kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt [...]."

Art. 6 Ziff. 1 lit. f) der DS-GVO geht in dieselbe Richtung. Er besagt, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, gegenüber dem berechtigten Interesse der verantwortlichen Stelle nicht überwiegen dürfen. Daneben sieht die DS-GVO ein ausdrückliches Widerspruchsrecht des Betroffenen vor, welches nur durch zwingende schutzwürdige Gründe für die Verarbeitung überwunden werden kann (Art. 19 Ziff. 1).

Es gibt wenig Hilfestellung für die Beantwortung der Frage, worin solche überwiegenden Interessen des Betroffenen im Kontext transkontinentaler Rechtsstreitigkeiten bestehen könnten. Generell gilt, dass die Privat- und Intimsphäre des Betroffenen zu schützen ist. Wirtschaftliche und berufliche Nachteile sowie Auswirkungen auf das Ansehen können ebenfalls relevante Faktoren sein.[81] Im Allgemeinen wird man eine summarische Interessenabwägung durch die verantwortliche Stelle ausreichen lassen.[82] Dabei wird in Fällen, in denen der Betroffene in angemessener Weise unterrichtet wurde und der Datenverwendung nicht widerspricht, für die verantwortliche Stelle – bei einer summarischen Prüfung[83] – kein Grund zu der Annahme bestehen, dass schutzwürdige Interessen des Betroffenen gegenüber ihrem berechtigten Interesse überwiegen. Indessen muss darüber hinaus die Datenverwendung stets noch verhältnismäßig sein.

Im Ergebnis ist damit eine Abwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und denen des Betroffenen („Interessenabwägung") erforderlich. Das entspricht nicht nur dem aktuellen Verständnis der Rechtslage, sondern wird auch bei Inkrafttreten der DS-GVO weiter gelten, wie sich aus dem Memorandum(2012) ableiten lässt. Dieses führt aus, dass der Export „unter bestimmten, eng umrissenen Umständen mit einem berechtigten Interesse des für die Verarbeitung Verantwortlichen [...] gerechtfertigt werden [kann]. Zuvor müssen die Umstände des Übermittlungsvorgangs allerdings geprüft [...] worden sein".[84]

Die Interessenabwägung erfordert die Berücksichtigung von Verhältnismäßigkeit, Prozesserheblichkeit und potenziellen Auswirkungen auf den Betroffenen.[85] Wie von der *Art. 29-Datenschutzgruppe* dargelegt, ist klar, dass „sowohl das US-Recht als auch die Rechtssysteme in der EU dem Verhältnismäßigkeitsgrundsatz und dem Ausgleich der verschiedenen Interessen Bedeutung beimessen."[86] Im Lichte der allgemeinen datenschutzrechtlichen Grundsätze, die sich aus § 3a BDSG ergeben – Datenvermeidung und Datensparsamkeit – ist die zulässige Datenverwendung auf die personenbezogenen Daten begrenzt, die unbedingt zur Verteidigung gegen die ausländische Klage erforderlich sind.[87] Die Abwägung der maßgeblichen Interessen verlangt dabei mehr als die bloße Minimierung der Datenmenge. Durch die Abwägung wird der verantwortlichen Stelle vielmehr abverlangt, dass sie bei der Verfolgung ihrer berechtigten Interessen so wenig personenbezogene Daten wie möglich verwendet und so wenig wie möglich in die Rechte der Betroffenen eingreift.[88]

Natürlich verlangt die Suche nach einer Lösung, die dem Grundsatz der Verhältnismäßigkeit entspricht, nach einer an den tatsächlichen Umständen des Einzelfalls orientierten Beurteilung mit Blick auf jeden Handlungsschritt. Diese Beurteilung wird bzgl. jeden Schritts der Datenverwendungskette in den folgenden Kapiteln durchgeführt.

c) Einbeziehung von Dienstleistungsunternehmen

In vielen Fällen wird die verantwortliche Stelle nicht über die Ressourcen oder das Know-How verfügen, um die personenbezogenen Daten selbst zu erheben, zu verarbeiten oder zu nutzen. Soweit es sich um Datenverwendungen durch die verantwortliche Stelle selbst handelt, können diese gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG auf Grund eigener Geschäftsinteressen zulässig sein. Soweit eine Datenverwendung durch die verantwortliche Stelle selbst hiernach zulässig ist und soweit kein Export stattfindet, kann auch die Datenverwendung im Auftrag durch ein auf Discovery-Verfahren spezialisiertes Dienstleistungsunternehmen auf diese Rechtsvorschrift gestützt werden. Dienstleistungsunternehmen innerhalb des Europäischen Wirtschaftsraums, die im Auftrag der verantwortlichen Stelle handeln, stehen in der Sphäre der verantwortlichen Stelle. Infolgedessen bedarf die

76 Die Frage, ob ein legitimes Interesse auch dann besteht, wenn sich die Klage nicht gegen die verantwortliche Stelle, sondern gegen eine mit ihr verbundene Gesellschaft richtet, wird nicht im Detail in dieser Veröffentlichung behandelt. *Brisch/Laue* führen jedoch aus, dass das berechtigte Interesse einer verbundenen Gesellschaft nicht ausreicht; *Brisch/Laue*, RDV 2010, 1, 4. Die *Art. 29-Datenschutzgruppe* scheint die Übermittlung durch die europäische Tochtergesellschaft einer beklagten ausländischen Muttergesellschaft zu erlauben; *Art. 29-Datenschutzgruppe*, WP 114, S. 15; *Hanloser*, DuD 2008, 785, 786, scheint dieser Ansicht folgen zu wollen.

77 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. EL 2011, § 28 BDSG Rdnr. 230; Däubler/*Wedde*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 28 Rdnr. 48.

78 *Brisch/Laue*, RDV 2010, 1, 4; *Spies/Schröder*, MMR 2008, 275, 278

79 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. EL 2011, § 28 BDSG Rdnr. 235; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 Rdnr. 108.

80 *Brisch/Laue*, RDV 2010, 1, 4.

81 *Gola/Schomerus*, BDSG, 10. Aufl. 2010, § 28 Rdnr. 35.

82 Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 BDSG Rdnr. 129.

83 Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 BDSG Rdnr. 129.

84 Memorandum(2012), S. 12.

85 *Brisch/Laue*, RDV 2010, 1, 6; *Art. 29-Datenschutzgruppe*, WP 158, S. 11.

86 *Art. 29-Datenschutzgruppe*, WP 158, S. 10.

87 Daten-Lagerung und Daten-Mining sind deshalb z.B. nicht umfasst; Däubler/*Wedde*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 28 Rdnr. 50.

88 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. EL 2011, § 28 BDSG, Rdnr. 239; Simitis/*Simitis*, BDSG, 7. Aufl. 2011, § 28 BDSG Rdnr. 129.

Weitergabe der Daten an den Auftragnehmer keiner eigenen Rechtsgrundlage.[89]

Gem. § 11 Abs. 2 BDSG muss die verantwortliche Stelle den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählen. Der Umfang, die Art und der Zweck der vorgesehenen Datenverwendung sind schriftlich festzulegen. Zusätzlich verlangen § 11 Abs. 2 Satz 4 und Satz 5 BDSG, dass die verantwortliche Stelle regelmäßig die Einhaltung der Vorgaben hinsichtlich des Datenschutzes überprüft und das Ergebnis ordnungsgemäß dokumentiert.

Auch die DS-GVO stellt entsprechende Anforderungen an die Auftragsverarbeitung. Speziell Art. 26 der DS-GVO lehnt sich im Wesentlichen an das gegenwärtig geltende deutsche Recht (§ 11 BDSG) an.

5. Spezifische Anforderungen an den Export personenbezogener Daten in die USA

Der zweite Teil des zweistufigen Ansatzes erfordert, dass die spezifischen Anforderungen zur Legitimierung eines Datenexports erfüllt werden. Der Grundgedanke hinter dem europäischen Datenschutzrecht verlangt, dass die Rechte und Interessen des Betroffenen durch den Export nicht gefährdet werden. Daher ist für personenbezogene Daten, die den sicheren europäischen Kokon verlassen, im Wesentlichen der innerhalb der EU geltende Schutzstandard beizubehalten. Zur Erreichung dieses Zwecks finden neben den allgemeinen datenschutzrechtlichen Grundsätzen die §§ 4b und 4c BDSG Anwendung,[90] die für den Datenexport zusätzliche Anforderungen aufstellen.[91]

Im Allgemeinen sollen personenbezogene Daten nicht in Drittstaaten (damit sind Nicht-EU- oder Nicht-EWG-Staaten gemeint) übermittelt werden, wenn ein solcher Drittstaat ein „angemessenes Datenschutzniveau" nicht gewährleistet.[92] Zum gegenwärtigen Zeitpunkt muss angenommen werden, dass die USA nicht das erforderliche Schutzniveau bieten.[93]

Allerdings bestehen nach dem BDSG im Grundsatz mehrere Möglichkeiten, um den Datenexport in die USA dennoch zu legitimieren. Die entsprechenden Instrumente sollen sicherstellen, dass der Betroffene im konkreten Einzelfall einen angemessenen Schutz genießt, obwohl im Zielland kein allgemeines „angemessenes Datenschutzniveau" besteht.

a) Grundsätze des „sicheren Hafens"

Mit der Entscheidung der *Europäischen Kommission* 2000/520/EG wurde im Wege einer Vereinbarung zwischen der *Kommission* und dem *US-Handelsministerium* ein spezifischer Weg geschaffen, den Datenexport in die USA zu erlauben. Ein angemessenes Schutzniveau wird dann als gewährleistet erachtet, wenn die Daten an Unternehmen und Organisationen mit Sitz in den USA übermittelt werden, welche die Grundsätze des „sicheren Hafens" zum Datenschutz befolgen und diese gemäß den in den vom *US-Handelsministerium* herausgegebenen „Häufig gestellten Fragen" (FAQ) enthaltenen Leitlinien umgesetzt haben (Art. 1 der EG-Entscheidung).

Während einige weltweit tätige Anwaltskanzleien (selbst-)zertifizierte „Sichere Häfen" darstellen,[94] scheint es unwahrscheinlich, dass sich die gegnerische Partei in einem US-Zivilrechtsstreit und US-Gerichte diesen Regeln unterwerfen können und werden.[95]

b) Übermittlungsvertrag

Falls der Drittstaat weder ein „angemessenes Datenschutzniveau" gewährleistet noch die Grundsätze des „sicheren Hafens" umgesetzt werden können, verbleibt die Möglichkeit, dass die zuständige nationale Aufsichtsbehörde die Datenübermittlung genehmigt. Dies setzt voraus, dass die verantwortliche Stelle ausreichende Garantien hinsichtlich des Datenschutzes und der Ausübung der damit verbundenen Rechte vorweist. § 4c Abs. 2 BDSG legt insoweit die verschiedenen Möglichkeiten dar.

Hiernach stellt ein Übermittlungsvertrag eine der Möglichkeiten zur Erbringung ausreichender Datenschutzgarantien dar. Die *EU-Kommission* hat in mehreren Entscheidungen Standardklauseln für solche Übermittlungsverträge erlassen.[96] In einer Pressemitteilung v. 7.1.2005 erklärte die *Kommission*, dass „Standardvertragsklauseln [...] ein Instrument [sind], mit dem Unternehmen und Organisationen auf unkomplizierte Weise ihren Verpflichtungen [...] nachkommen können, wonach sie personenbezogene Daten, die in Nicht-EU-Länder übermittelt werden, angemessen schützen müssen."[97] Die Aufsichtsbehörden der Mitgliedstaaten müssen anerkennen, dass diese Übermittlungen einen angemessenen Datenschutz gewährleisten.[98]

Obwohl § 4c Abs. 2 Satz 1 BDSG nach seinem Wortlaut nahelegt, dass eine Genehmigung erforderlich ist, nimmt eine Mehrzahl der Kommentatoren offensichtlich an, dass die bloße Unterrichtung der nationalen Aufsichtsbehörde ausreiche und dass, solange die Standardvertragsklauseln in unmodifizierter Form verwendet werden, keine zusätzlichen Anforderungen bestehen. Folgt man dieser Auffassung, dann ist sogar das Erfordernis der Unterrichtung der zuständigen Aufsichtsbehörde verzichtbar und würde vielmehr wahrscheinlich sogar gegen den Verhältnismäßigkeitsgrundsatz verstoßen.[99]

Aus Praxissicht scheint es jedoch ratsam, die Auffassung der zuständigen Aufsichtsbehörde bzgl. etwaiger Unterrichtungs- und Genehmigungserfordernisse in diesem Zusammenhang zu erfragen. Angeblich vertreten einige Aufsichtsbehörden außerhalb Deutschlands eine hiervon abweichende, strengere Haltung. Daher wird vorgeschlagen, die nationale Aufsichtsbehörde entsprechend zu unterrichten und dabei ausdrücklich zu erklären, man gehe davon aus, eine Genehmigung sei nicht erforderlich, sowie die Aufsichtsbehörde um Mitteilung für den Fall zu bitten, dass sie eine andere Auffassung vertreten sollte. Selbstverständlich sollte eine Rückantwortfrist gesetzt werden und vor deren Ablauf kein Export erfolgen.

Wird von den Standardvertragsklauseln abgewichen, ist indessen eine gesonderte Erlaubnis der Aufsichtsbehörde erforderlich. Vor der Übermittlung personenbezogener Daten ist zu verifizieren, dass der ausländische Empfänger nicht in seinem Land zu Verstößen gegen den Übermittlungsvertrag gezwungen werden kann. Falls ein solcher Nachweis fehlschlägt, folgt hieraus, dass der Übermittlungsvertrag den betreffenden Export nicht legitimieren kann.[100]

---

89 § 3 Abs. 8 Satz 3 BDSG.
90 Vgl. unter III.4 und III.8 bzgl. besonderer Arten personenbezogener Daten.
91 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. EL 2011, § 4c BDSG Rdnr. 19.
92 § 4b Abs. 2 Satz 2 BDSG.
93 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4b Rdnr. 15; *Brisch/Laue*, RDV 2010, 1, 6; *Spies*, MMR 7/2007, S. V, VII; *TSC*, International Overview 2009 – Deutschland, S. 102. Zudem wäre die Entscheidung der *EU-Kommission* 2000/520/EG gänzlich überflüssig, würde man glauben, die USA böten das geforderte Schutzniveau.
94 Die Liste ist abrufbar unter: https://safeharbor.export.gov/list.aspx.
95 *Brisch/Laue*, RDV 2010, 1, 6; *Hanloser*, DuD 2008, 785, 788.
96 S. 2001/497/EG, 2002/16/EG (widerrufen durch 2010/87/EU), 2004/915/EG und 2010/87/EU.
97 PM der *EU-Kommission*, IP/05/12.
98 S. Entscheid der *EU-Kommission* 2010/87/EU, Erwägungsgrund 5; Memo der *EU-Kommission*, Memo/10/30, S. 1.
99 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. EL 2011, § 4c BDSG Rdnr. 23; Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4c Rdnr. 18c m.w.Nw.
100 Eine solche Bewertung hinsichtlich der USA liegt außerhalb des Umfangs dieser Veröffentlichung.

Zusammenfassend lässt sich sagen, dass der Abschluss eines Übermittlungsvertrags, was Übermittlungen an einen externen Rechtsanwalt oder ein Dienstleistungsunternehmen im Ausland betrifft, einen brauchbaren Ausgangspunkt bietet.[101] Nach Ansicht einiger Kommentatoren stellt ein solcher Übermittlungsvertrag sogar den Regelfall in Bezug auf die verantwortlichen Stellen und ihre externen Rechtsanwälte dar.[102] In diesem Zusammenhang ist darauf hinzuweisen, dass die *Art. 29-Datenschutzgruppe* die Ansicht vertritt, dass „sichere Häfen", Übermittlungsverträge oder internationale Übereinkommen gegenüber gesetzlichen Ausnahmeregelungen, die unten diskutiert werden, zu bevorzugen seien.[103] Für Übermittlungen, die als wiederholt, gehäuft oder routinemäßig eingestuft werden können, sollte hiernach bevorzugt ein solcher spezifischer rechtlicher Rahmen zum Einsatz gebracht werden.[104]

Wie dem auch immer sei, es erscheint jedenfalls als unwahrscheinlich, dass die Rechtsanwälte des Prozessgegners oder US-amerikanische Gerichte imstande oder gewillt sind, entsprechende Übermittlungsverträge abzuschließen.[105]

c) Verbindliche Unternehmensrichtlinien

Konzerne können verbindliche Unternehmensrichtlinien (Binding Corporate Rules – BCR) aufstellen, um einen angemessenen Datenschutz für den Datenexport zu gewährleisten. BCR werden im BDSG ausdrücklich als Möglichkeit der verantwortlichen Stelle genannt, ausreichende Schutzgarantien vorzuweisen, wie dies von § 4c Abs. 2 Satz 1 BDSG verlangt wird.[106]

Die BCR müssen sowohl intern im Konzern als auch nach außen verbindlich sein. In der Regel müssen die BCR ein vergleichbares Datenschutzniveau wie die Übermittlungsverträge gewährleisten, da sie letztlich als konzerninterne Übermittlungsverträge anzusehen sind.[107] BCR sind jedoch nur für Datenübermittlungen innerhalb eines Konzerns verwendbar.[108]

Ein Datenexport auf der Grundlage von BCR bedarf der Genehmigung der zuständigen Aufsichtsbehörde.[109] § 4c Abs. 2 Satz 1 BDSG legt fest, dass eine Genehmigung erforderlich ist. Angesichts des Umstands, dass es bislang keine gesetzlichen Standards für BCR gibt, handelt es sich dabei auch nicht um eine bloße Formalie. Obwohl die BCR selbst nicht genehmigungsbedürftig sind, hat sich zwischen den nationalen Aufsichtsbehörden ein informelles Verfahren zur Abstimmung von BCR etabliert. Die einzelstaatlichen Behörden vergleichen dabei das Datenschutzniveau nach Maßgabe der DS-RL mit den BCR und stellen auf diesem Wege fest, ob angemessene Schutzgarantien nachgewiesen sind.

Einige weltweit operierende Unternehmensgruppen verfügen über solche BCR.[110] Allerdings bieten BCR keine Möglichkeit, um den Export von einer europäischen verantwortlichen Stelle, die als Partei in einem US-Zivilprozess auftritt, an ihre externen Rechtsanwälte in den USA zu legitimieren.

d) Erfüllung gesetzlicher Anforderungen

Eine weitere Möglichkeit eröffnet Art. 26 Abs. 1 lit. d) der DS-RL. Danach soll der Export rechtmäßig sein, wenn die Datenübermittlung „für die Wahrung eines wichtigen öffentlichen Interesses [...] erforderlich oder gesetzlich vorgeschrieben ist."

Das BDSG setzt die Ausnahmealternative des „gesetzlich vorgeschriebenen" Datenexports nicht ausdrücklich um.[111] Um die Vorgaben der DS-RL zu erfüllen, wird vorgeschlagen, diese Option im Wege der Auslegung in das Merkmal der Erforderlichkeit zur „Wahrung eines wichtigen öffentlichen Interesses" i.S.d. § 4c Abs. 1 Nr. 4 BDSG hineinzulesen. [112]

Gesetzliche Verpflichtungen, die sich aus einem ausländischen Gesetz oder einer ausländischen Rechtsvorschrift ergeben, sind nicht als gesetzliche Verpflichtung i.S.d. Regelung anzusehen, durch welche der Export erlaubt werden könnte. Dasselbe gilt für eine ausländische Gerichtsentscheidung. Datenschutz innerhalb der EU kann nicht von der Gesetzgebung von Nicht-EU-Staaten abhängig gemacht werden. Die maßgebliche Entscheidung darüber, ob ein zu wahrendes wichtiges öffentliches Interesse vorliegt, ist durch die nationale Gesetzgebung, welcher die verantwortliche Stelle in der EU unterliegt, zu treffen, und nicht durch ausländische Hoheitsträger.[113] Die DS-GVO stellt dies noch klarer heraus, indem sie explizit verlangt, dass die gesetzliche Verpflichtung sich aus dem „Unionsrecht oder Recht des Mitgliedsstaates" ergeben muss,[114] selbst wenn das ausländische Recht „die Datenverarbeitungstätigkeiten [...] unmittelbar reguliert".[115]

Die Befolgung von Anfragen, die im Einklang mit dem Haager Übereinkommen über die Beweisaufnahme im Ausland in Zivil- oder Handelssachen v. 18.3.1970 (Haager Beweisübereinkommen – HBÜ) gestellt werden, könnte theoretisch eine formelle Rechtsgrundlage für den Export personenbezogener Daten darstellen. Das HBÜ regelt Verfahren der Zusammenarbeit für die Beweisaufnahme im Ausland und gilt nur zwischen den Unterzeichnerstaaten. Ein Vertragsstaat kann durch Rechtshilfeersuchen die zuständige Behörde eines anderen Vertragsstaats ersuchen, eine Beweisaufnahme vorzunehmen. Die *Art. 29-Datenschutzgruppe* erklärte, dass wenn möglich zuerst das HBÜ in Betracht gezogen werden sollte, um den Export von Daten zu Prozesszwecken zu ermöglichen.[116]

Zwar lässt das HBÜ an sich das Ersuchen für eine pre-trial Discovery zu. Jedoch haben zahlreiche Vertragsstaaten, wie z.B. Deutschland, Frankreich, Spanien und die Niederlande, im Einklang mit Art. 23 des HBÜ erklärt, „dass [sie] Rechtshilfeersuchen nicht erledig[en], die ein Verfahren zum Gegenstand haben, das in den Ländern des „Common Law" unter der Bezeichnung „pre-trial discovery of documents" bekannt ist."[117] Aus diesem Grund werden die zuständigen deutschen Behörden generell Ersuchen um die Vorlage von Unterlagen in Discovery-Ver-

---

101 *Brisch/Laue*, RDV 2010, 1, 6.
102 *Spies/Schröder*, MMR 2008, 275, 279.
103 S. unter III.5.d) und III.5.e).
104 *Art. 29-Datenschutzgruppe*, WP 114, S. 9.
105 *Brisch/Laue*, RDV 2010, 1, 6.
106 Nach anderer Auffassung führen BCR zu einem angemessenen Datenschutzniveau i.S.d. § 4b Abs. 2 Satz 3 BDSG. Entsprechende Exporte benötigten dann keine Genehmigung.
107 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4c Rdnr. 22; *Hanloser*, DuD 2008, 785, 788.
108 *Hanloser*, DuD 2008, 785, 788; nach *Däubler* ist insoweit § 15 AktG ausschlaggebend, Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4c Rdnr. 24.
109 *Kunert*, 11 PVLR 06, 9 unterstellt, dass gegenwärtig spezifische Genehmigungen erforderlich sind, weil deren Wegfall ein „great boon" ist.
110 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 4c Rdnr. 24; der angeführte Link konnte jedoch nicht verifiziert werden.
111 Am Rande: Die vom *BfDI* gestellte Übersetzung spiegelt die Unterschiede zwischen der DS-RL und dem BDSG nicht wider, abrufbar unter: http://www.bfdi.bund.de/cae/servlet/contentblob/844438/publicationFile/51362/aktualisiertesBDSG.pdf.
112 Die deutsch-sprachigen Fassungen lauten:
Art. 26 Abs. 1 lit. d der RL:
„die Übermittlung [...] für die Wahrung eines wichtigen öffentlichen Interesses [...] erforderlich oder gesetzlich vorgeschrieben ist."
§ 4c Abs. 1 Satz 4 BDSG:
„die Übermittlung [...] für die Wahrung eines wichtigen öffentlichen Interesses [...] erforderlich ist."
113 *Art. 29-Datenschutzgruppe*, WP 114, S. 15; *Art. 29-Datenschutzgruppe*, WP 158, S. 9.
114 DS-GVO, Art. 6 Abs. 1 lit. c und Abs. 3.
115 DS-GVO, Erwägungsgründe 78 und 90.
116 *Art. 29-Datenschutzgruppe*, WP 158, S. 14.
117 S. § 14 des Ausführungsgesetzes zu den Haager Reformübereinkommen von 1965 und 1970.

fahren nach dem HBÜ nicht nachkommen.[118] Daher kann das HBÜ derzeit nicht als Rechtsgrundlage für einen rechtmäßigen Export personenbezogener Daten, die dem deutschen Datenschutzrecht unterliegen, in die USA herangezogen werden. Es ist auch zu beachten, dass die Schutzgarantien, die das HBÜ bietet, ohnehin in den USA kaum Wirkung entfalten.[119]

Indessen könnten Modifikationen des HBÜ oder des deutschen Umsetzungsgesetzes de lege ferenda das Dilemma, das den Gegenstand der vorliegenden Veröffentlichung bildet, abmildern. Auch wenn sich dies lange hinziehen würde und großer Anstrengungen bedürfte, könnte es der Mühe wert sein. Dies gilt insbesondere insofern, als durch eine Modifizierung des HBÜ zwei Ziele erreicht werden könnten: die Schaffung einer Rechtsgrundlage für den Export personenbezogener Daten in die USA für transkontinentale Rechtsstreitigkeiten sowie die umfassende Anerkennung und Umsetzung des Übereinkommens in den USA. Auf internationaler Ebene sollten Diskussionsrunden und Konsultationen für das HBÜ II begonnen werden.[120]

e) Erforderlichkeit in Bezug auf Rechtsansprüche vor Gericht

Eine weitere Option zur Legitimierung des Exports in einen Drittstaat findet sich in § 4 Abs. 1 Nr. 4 BDSG. Diese gesetzliche Ausnahmeregelung greift in dem Fall, dass „die Übermittlung [...] zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist."

Die Vorschrift spiegelt die Auffassung des Gesetzgebers wider, dass die Fähigkeit der verantwortlichen Stelle, ihre Rechte geltend zu machen oder zu verteidigen, nicht unnötig eingeschränkt werden sollte. Auch wenn noch keine Entscheidungen deutscher Gerichte hierzu vorliegen,[121] ist doch davon auszugehen, dass die „Ausnahmeregelung im Zusammenhang mit Rechtsansprüchen" nicht nur die Übermittlung von personenbezogenen Daten an das Gericht, sondern auch an alle anderen Stellen erfasst, die in das Gerichtsverfahren involviert sind, da sie sonst leerliefe.[122]

Liest man die Vorschrift, so könnte man sich fragen, ob durch sie im Kontext ausländischer Gerichtsverfahren überhaupt eine zusätzliche Anforderung aufgestellt werden soll. Die (weitergefasste) für Datenverwendungen geltende allgemeine gesetzliche Voraussetzung gem. § 28 BDSG lässt eine Verwendung personenbezogener Daten zu, „[...] soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist [...]." Zweifellos stellen die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht berechtigte Interessen in diesem Sinne dar.

Das Zusammenspiel der beiden Vorschriften erklärt sich mit Hilfe folgender Erwägungen: Aus datenschutzrechtlicher Sicht wird der Export personenbezogener Daten in Drittstaaten mit einem weniger strengen Datenschutzsystem als das der EU-Mitgliedstaaten grundsätzlich missbilligt. In diesem Zusammenhang stellt § 4c Abs. 1 BDSG eine Ausnahme vom allgemeinen Grundsatz dar, dass der Export in Drittstaaten nur erfolgen darf, wenn ein angemessenes Datenschutzniveau auf anderem Wege gewährleistet ist. Die Ausnahmevorschrift erkennt also an, dass die Ausweitung des Welthandels unter gewissen Umständen Flexibilität erfordert.[123] Allerdings ist die Ausnahme eng auszulegen und in einer Weise anzuwenden, die das Fehlen eines angemessenen Schutzniveaus kompensiert.[124]

Auch wenn einige Stimmen aus der Literatur die Ansicht vertreten, dass die Interessen des Betroffenen in der Regel gegen den Export sprechen,[125] widerspräche solch ein weitgehender Ansatz dem anerkannten Bedürfnis nach Flexibilität im Welthandel. Überdies könnte sich ein solcher Ansatz für den Schutz personenbezogener Daten sogar als schädlich erweisen. Dies wäre etwa dann der Fall, wenn das betreffende US-Gericht zu dem Ergebnis käme, dass die nationalen Datenschutzbestimmungen als „Sperrgesetz" einzustufen wären und es diese daher für schlechterdings unbeachtlich erklärte. Die Suche nach wechselseitig akzeptablen Lösungen erfordert es gemäß dem TSC International Principle I stattdessen, dem jeweils anderen Rechtssystem angemessene Achtung entgegenzubringen.[126] Daher sehen die meisten Quellen § 4c Abs. 1 Nr. 4 BDSG – in restriktiver Auslegung – zutreffend als Erlaubnistatbestand für die Übermittlung personenbezogener Daten an die eigenen Rechtsanwälte, an Dienstleistungsunternehmen, die Rechtsanwälte der Gegenseite und das Gericht an.[127]

Um die gebotene restriktive Anwendung des § 4c Abs. 1 Nr. 4 BDSG bzw. die Verhältnismäßigkeit speziell des Exports zu gewährleisten, ist eine zusätzliche exportbezogene Interessenabwägung („Export-Abwägung") durchzuführen, die der Abwägung zur Erfüllung der allgemeinen Datenverwendungsvoraussetzungen nach § 28 BDSG ähnelt.[128] Dabei ist nunmehr der Umstand zu berücksichtigen, dass die Übermittlung personenbezogener Daten in ein Land, das kein angemessenes Datenschutzniveau gewährleistet, bedeutet, dass die Persönlichkeitsrechte des Betroffenen in einem höheren Maße gefährdet werden. Als Beispiel sei insoweit nur auf den Umstand verwiesen, dass soweit keine anderslautende gerichtliche Anordnung vorliegt, in den USA die Gerichtsakte allgemein für die Öffentlichkeit zugänglich ist.[129] Dies steht in deutlichem Gegensatz zu den Vorstellungen des EU-Datenschutzrechts. Deshalb ist die Schwelle für die Zulässigkeit des Exports personenbezogener Daten in solche Staaten gegenüber Datenübermittlungen innerhalb des EWR zu erhöhen; die Waagschale neigt sich – bildlich gesprochen – zu Ungunsten der Übermittlung.

6. Export-Abwägung

Das letzte Kapitel endete mit der Schlussfolgerung, dass eine Export-Abwägung durchzuführen ist, wenn die Ausnahmeregelung in Bezug auf Rechtsansprüche in Anspruch genommen

---

118 *Hanloser*, DuD 2008, 785, 786. Der auf Deutschland bezogene Teil des *TSC*, International Overview of Discovery, Data Privacy & Disclosure Requirements führt auf S. 95 aus, dass die deutschen zuständigen Stellen in manchen Fällen die Rechtshilfeersuchen an die zuständigen Amtsgerichte weiterleiten, wenn ein US-amerikanisches Gericht bestimmte Dokumente von der Partei oder einem Dritten in Deutschland anfordert, die Dokumente entscheidungserheblich sind und das Verfahren in den USA bereits rechtshängig ist. Jegliche derartige Unterstützung verletze jedoch deutsches Recht, da die Rechtsverordnung nach § 14 Abs. 2 des Ausführungsgesetzes nicht erlassen wurde.

119 Dies liegt daran, dass (a) Gerichte in den USA die Einhaltung der HBÜ nicht für zwingend erforderlich halten, da diese einen, aber nicht den einzigen, Weg darstellt, Beweismittel im Ausland zu erlangen. Demnach ist das HBÜ eine Option, welche die Kläger nutzen können. Dadurch wird das HBÜ im Wesentlichen sinnlos (*Art. 29-Datenschutzgruppe*, WP 158, S. 7); (b) Beklagte häufig „freiwillig" mit den Kläger kooperieren um negative Implikationen in US-amerikanischen Verfahren zu vermeiden; und (c) Beklagte häufig selbst die Vorlage von Unterlagen verlangen, s. *Art. 29-Datenschutzgruppe*, WP 158, S. 9.

120 *Knöfel* führt aus, dass Discovery-Ersuchen regelmäßig i.R.d. HBÜ abgehandelt werden sollten, RIW 2010, 403, 406.

121 *TSC*, International Overview 2009 – Deutschland, S. 103.

122 *Spies/Schröder*, MMR 2008, 275, 279; *TSC*, International Overview 2009 – Deutschland, S. 103.

123 RL, Erwägungsgrund 58.

124 Taeger/*Gabel*, BDSG, § 4c Rdnr. 5; im Hinblick auf die RL *Art. 29-Datenschutzgruppe*, WP 114, S. 7.

125 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. EL 2011, § 28 BDSG Rdnr. 245.

126 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, S. 7.

127 *Brisch/Laue*, RDV 2010, 1, 7; *Spies/Schröder*, MMR 2008, 275, 279; *Hanloser*, DuD 2008, 785, 788 et. al.; für die gegenteilige Ansicht s. Fußn. 125.

128 S. unter III.4.b).

129 *Rath/Klug*, K&R 2008, 596, 598.

wird. Diese Voraussetzung betrifft jedoch nicht nur die „Rechtsanspruchs-Ausnahme", sie gilt vielmehr auch in den Fällen der Berufung auf einen „sicheren Hafen" oder einen Übermittlungsvertrag.

Auch wenn eine verantwortliche Stelle, die sich beim Datenexport auf die Grundsätze des „sicheren Hafens" beruft oder Übermittlungsverträge nutzt und hierdurch beim Empfänger allgemein ein „angemessenes Datenschutzniveau" bzw. „ausreichende Datenschutzgarantien" gewährleistet, kann der Betroffene nichtsdestotrotz ein berechtigtes Interesse daran haben, die Möglichkeit eines Exports auszuschließen. Der Wortlaut von § 4b Abs. 2 Satz 2 BDSG bietet einen ersten Anhaltspunkt für dieses Ergebnis: Ein solches schutzwürdiges Interesse kann danach „insbesondere" dann bestehen, wenn ein angemessenes Datenschutzniveau nicht gewährleistet ist. Der Wortlaut der Vorschrift lässt damit erkennen, dass es daneben auch andere Gründe geben kann. Außerdem wurde bereits oben dargelegt, dass solche Exporte grundsätzlich missbilligt werden.[130] Ferner geht die DS-RL (Art. 25 Ziff. 1) davon aus, dass neben dem Vorliegen der allgemeinen und spezifischen Voraussetzungen für einen konkreten Export auch das allgemeine Datenschutzniveau im Drittland zu beurteilen ist. Ohne die Export-Abwägung wäre dies nicht gewährleistet.

Aus diesen Gründen steht eine unbeschränkte Übermittlung aller personenbezogenen Daten in die USA im Widerspruch zum deutschen und europäischen Datenschutzrecht, selbst wenn die allgemeinen Datenverwendungsvoraussetzungen und die formellen exportspezifischen Anforderungen erfüllt sind. Die Export-Abwägung muss jedem Export vorausgehen, um diesen legitimieren zu können. Die Besonderheiten der Export-Abwägung werden im Kontext des entsprechenden Schritts der Datenverwendungskette diskutiert.

7. DS-GVO: Export-Abwägung weiterhin erforderlich

Auch die DS-GVO folgt weiterhin dem zweistufigen Ansatz, wie ihrem Art. 40 zu entnehmen ist: allgemeine sowie besondere Anforderungen sind einzuhalten. Auf der allgemeinen Ebene ist die Datenverwendung rechtmäßig, wenn sie „zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen."[131] Damit muss auch hiernach eine Interessenabwägung durchgeführt und „bestanden" werden, damit eine Datenverwendung im Licht dieser allgemeinen Voraussetzung als zulässig angesehen werden kann.

Was das Erfordernis einer Export-Abwägung anbelangt, ist der Wortlaut weniger deutlich. Die DS-GVO hält drei Optionen für einen rechtmäßigen Export bereit:

- einen Angemessenheitsbeschluss in Bezug auf das Drittland,[132] welcher hinsichtlich der USA weder aktuell vorhanden ist noch in absehbarer Zeit zu erwarten steht;[133]
- angemessene Schutzgarantien durch ein rechtlich verbindliches Instrument oder durch eine vorherige Genehmigung der zuständigen Aufsichtsbehörde[134] oder
- eine Ausnahme für den Fall, dass der Export „erforderlich ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht".[135]

Es gibt somit keinen Hinweis darauf, dass durch Inkrafttreten der DS-GVO die gegenwärtigen allgemeinen und spezifischen Export-Voraussetzungen aufgeweicht werden könnten.

Eher dürfte das Gegenteil der Fall sein. Das lässt sich anhand der Änderungen belegen, die vor der Veröffentlichung der DS-GVO noch kurzfristig vorgenommen wurden. Aus dem Memorandum zur internen Entwurfsfassung 56 der Verordnung ging auf S. 12 hervor, dass es gem. Art. 42 dieser Fassung einer verantwortlichen Stelle verboten sein sollte, auf das Ersuchen eines Gerichts oder einer Verwaltungsbehörde eines Drittstaats hin personenbezogene Daten in diesen Drittstaat zu übermitteln, sofern dies nicht ausdrücklich durch ein internationales Übereinkommen, durch gegenseitige Rechtshilfevereinbarungen oder durch Genehmigung der Aufsichtsbehörde gestattet ist. Ein entsprechender Artikel ist zwar nicht in die DS-GVO aufgenommen worden, die *Kommission* hat jedoch öffentlich erklärt, dass sie in Bezug auf Datenübermittlungen, welche von ausländischen Gerichten oder Regierungsbehörden angeordnet werden, Einschränkungen erwägt.[136] Die allgemeine Tendenz der *Kommission* ist klar: Der Export in die USA zu Prozesszwecken ist nicht gern gelitten und die hierfür zu erfüllenden Anforderungen werden nicht gelockert.

Es ist daher unwahrscheinlich, dass die *Kommission* ein Interesse daran hat, die spezifische Export-Abwägung zu verwerfen. Diese Ansicht lässt sich auf das Memorandum(2012) stützen, in dem es ausdrücklich heißt: „Der Datentransfer kann darüber hinaus unter bestimmten, eng umrissenen Umständen mit einem berechtigten Interesse des für die Verarbeitung Verantwortlichen [...] gerechtfertigt werden. Zuvor müssen die Umstände des Übermittlungsvorgangs allerdings geprüft und dokumentiert worden sein." Diese Aussage stellt einen weiteren Hinweis darauf dar, dass die Export-Abwägung auch in der Zukunft erforderlich sein wird. Zur Förderung dieses Ziels wird an dieser Stelle vorgeschlagen, den entsprechenden Wortlaut in die Endfassung der Verordnung oder wenigstens das entsprechende Memorandum aufzunehmen.

8. Der Umgang mit besonderen Arten personenbezogener Daten für transkontinentale Rechtsstreitigkeiten

Besondere Arten personenbezogener Daten genießen einen besonderen Schutz auf Grund des gesteigerten schutzwürdigen Interesses der Betroffenen.[137] Falls solche Daten im Zusammenhang mit transkontinentalen Rechtsstreitigkeiten verwendet werden, verdrängt § 28 Abs. 6 bis 9 BDSG die Regelung des § 28 Abs. 1 BDSG.

§ 28 Abs. 6 Nr. 3 BDSG erlaubt die Datenverwendung auf der ersten, allgemeinen Stufe, wenn „dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt". Aus diesem Grund kann die „Erforderlichkeit in Bezug auf Rechtsansprüche" grundsätzlich sogar zur Verwendung besonderer Arten personenbezogener Daten berechtigen, solange die Datenverwendung verhältnismäßig ist. In diesem Fall muss die Interessenabwägung sowohl der besonderen Sensibilität der Daten als auch dem Willen des EU-Gesetzgebers Rechnung tragen,[138] Daten dieser Art besonders zu schützen.

---

130 S. unter III.5.
131 DS-GVO, Art. 6 Abs. 1 lit. f.
132 DS-GVO, Art. 41 Abs. 1.
133 In Übereinstimmung mit DS-GVO, Art. 41 Abs. 5 und Abs. 6 kann die *EU-Kommission* eine Nicht-Angemessenheitsentscheidung treffen. In diesem Fall sind Datenübermittlungen verboten, vorbehaltlich der Regelung in den Art. 42 bis 44.
134 DS-GVO, Art. 42 Abs. 1.
135 DS-GVO, Art. 44 Abs. 1. lit. e.
136 *Kunert*, 11 PVLR 06, 10.
137 S. unter II.5.
138 Däubler/*Wedde*, BDSG Kompaktkommentar, 3. Aufl. 2010, § 28 Rdnr. 175.

Auf der zweiten, exportbezogenen Prüfungsstufe kann der Export besonderer Arten personenbezogener Daten unter spezifischen Voraussetzungen, insbesondere gem. § 4c Abs. 1 Nr. 4 BDSG, erlaubt sein. Die erforderliche Export-Abwägung muss ebenfalls das besondere Schutzbedürfnis berücksichtigen.

Insgesamt ist die besondere Notwendigkeit des Schutzes besonderer Arten personenbezogener Daten bei der Beurteilung jedes einzelnen Schritts der Datenverwendungskette und bei der Implementierung besonderer Schutzmaßnahmen zu berücksichtigten.

9. Einbeziehung des Datenschutzbeauftragten

Auch wenn das BDSG hierzu nicht ausdrücklich verpflichtet,[139] sollte es in Discovery-Fällen doch regelmäßig „Standard" sein, den Datenschutzbeauftragten der verantwortlichen Stelle aktiv einzubeziehen. Wenn der Datenschutzbeauftragte von einer speziellen Angelegenheit Kenntnis erhält und einbezogen werden möchte, ist er dazu berechtigt. Die Einbeziehung hat den Vorteil, dass der Datenschutzbeauftragte mit der nationalen Aufsichtsbehörde Rücksprache halten kann, um sicherzustellen, dass nicht gegen das nationale Datenschutzrecht verstoßen wird.[140] Darüber hinaus könnte es einem US-Gericht ungewöhnlich erscheinen, wenn die Unterstützung des Datenschutzbeauftragten nicht in Anspruch genommen wird, während andererseits seine Mitwirkung und sein „Segen" das Verhalten der verantwortlichen Stelle im Falle eines Discovery-Streits in ein positives Licht rücken könnte. Sicherlich ist die Einbeziehung ein Indiz dafür, dass die verantwortliche Stelle nach Treu und Glauben vorgegangen ist, was dann von Vorteil sein kann, wenn das US-Gericht oder eine nationale Aufsichtsbehörde dieses Vorgehen in Frage stellen sollte.

Obwohl die Einbeziehung des Datenschutzbeauftragten somit nicht zwingend vorgeschrieben ist, ist es doch angezeigt, ihn so rasch wie vernünftigerweise möglich zu beteiligen. Sollte die DS-GVO in der derzeitigen Fassung in Kraft treten, wird eine solche Einbeziehung vorgeschrieben sein.[141]

10. Transparenz

Nach Ansicht der *Art. 29-Datenschutzgruppe* verlangt die DS-RL eine allgemeine Unterrichtung im Voraus, wenn die Möglichkeit der Verwendung personenbezogener Daten zu Prozesszwecken besteht. Kommt es tatsächlich dazu, muss die Unterrichtung Auskunft über die Identität aller Empfänger, den Verwendungszweck, die Art der betroffenen personenbezogenen Daten und die Rechte des Betroffenen geben.[142]

Ein solches allgemeines Erfordernis ist wohl zu weitgehend und in dieser allgemeinen Form nicht handhabbar. Genauso schwierig, wie die Einwilligung aller Betroffenen in einem großen Verfahren zu erlangen, dürfte es auch sein, alle Betroffenen in angemessener Form zu unterrichten. Daher müssen die Spezifika dieses Erfordernisses im Hinblick auf jeden einzelnen Schritt der Datenverwendungskette bestimmt werden.

11. Rechte auf Auskunft, Berichtigung und Löschung

Sobald sie unterrichtet sind, haben Betroffene unter bestimmten Voraussetzungen ein Recht auf Auskunft über ihre personenbezogenen Daten sowie auf Berichtigung und Löschung. Die *Art. 29-Datenschutzgruppe* stellt zutreffend fest, dass „sich aus diesen Rechten ein Konflikt mit den prozessualen Anforderungen ergeben könnte, zu einem bestimmten Zeitpunkt gesicherte Daten unverändert aufzubewahren, da Datenänderungen (wenn auch nur für Berichtigungszwecke) eine Änderung der Beweismittel in der Streitsache bewirken würden".[143] Jedoch sollten sich in Zusammenarbeit mit der gegnerischen Partei und, falls notwendig, dem zuständigen US-Gericht Lösungen für dieses Problem finden lassen.

Aus praktischer Sicht sollten die betreffenden personenbezogenen Daten in Übereinstimmung mit TSC International Principle 4 von den übrigen Daten abgesondert werden,[144] sobald eine Berichtigungs- oder Löschungsanfrage vorliegt. Anschließend sollte eine Lösung mit dem Gegner ausgehandelt oder eine Entscheidung des US-Gerichts beantragt werden.

12. Datensicherheit

Die verantwortliche Stelle muss zumutbare technische und organisatorische Maßnahmen treffen, um die Sicherheit der personenbezogenen Daten zu gewährleisten und dadurch ein ausreichendes Datensicherheitsniveau sicherzustellen. Die Sicherheitsstufe muss den Risiken entsprechen, die im Einzelfall bestehen.[145] Die verantwortliche Stelle muss diese Anforderungen auch den Rechtsanwaltskanzleien, Dienstleistungsunternehmen und anderen Stellen, die mit den personenbezogenen Daten in Berührung kommen, auferlegen. Die verantwortliche Stelle ist auch für die Datenverarbeitung bei externen Dienstleistern verantwortlich und muss sich regelmäßig von der Einhaltung der Datensicherheitsmaßnahmen überzeugen.[146]

Gleiches könnte auch in Bezug auf die Gerichte gelten, „da ein Großteil der relevanten personenbezogenen Daten, die für den Ausgang des Verfahrens erheblich sind, bei diesen aufbewahrt werden."[147] Eine solche Anforderung weist der verantwortlichen Stelle eine interessante Aufgabe zu. Jedoch dürfte die verantwortliche Stelle insoweit i.E. nur dazu verpflichtet sein, das betreffende US-Gericht um angemessene Sicherheit zu ersuchen. In jedem Fall sollte es die entsprechenden Schritte und Bemühungen dokumentieren.

13. Dokumentation

Obschon erst die DS-GVO erhebliche und detaillierte Dokumentationspflichten aufstellt, sind verantwortliche Stellen schon unter dem geltenden BDSG gut beraten, Dokumentationsrichtlinien zu etablieren. Die Anwendung allgemeiner Unternehmensrichtlinien und die entsprechende Dokumentation ihrer Einhaltung belegen Treu und Glauben der verantwortlichen Stelle und können dabei helfen, ihr Vorgehen gegenüber nationalen Aufsichtsbehörden oder den US-Gerichten zu verteidigen.

IV. Anwendung I: Sicherung

Die im Hinblick auf den Umgang mit personenbezogenen Daten zu Zwecken transkontinentaler Gerichtsverfahren entwickelten Prinzipien und Grundregeln können nun zum Leben erweckt werden. Die folgenden Kapitel behandeln ihre praktische Anwendung i.R.d. einzelnen Schritte der Datenverwendungskette.

Die Sicherung stellt schon eine Datenverwendung dar, namentlich in der Terminologie des BDSG eine „Speicherung" gem. § 3 Abs. 4 Satz 2 Nr. 1 BDSG. Diese ist jedoch weitgehend, einschließlich der Erstellung einer Sicherungskopie, zulässig. Umfang und Beginn der legitimen Sicherung orientieren sich dabei

139 Sofern *Spies*, MMR 7/2007, S. V, VII eine Pflicht postuliert, den betrieblichen Datenschutzbeauftragten einzubeziehen, wird dem nicht zugestimmt.
140 *TSC*, International Overview 2009 – Deutschland, S. 101; im gleichen Sinne *Art. 29-Datenschutzgruppe*, WP 158, S. 11.
141 DS-GVO, Art. 36.
142 *Art. 29-Datenschutzgruppe*, WP 158, S. 11.
143 *Art. 29-Datenschutzgruppe*, WP 158, S. 12.
144 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, S. 17.
145 Explizit ist dies in DS-GVO, Art. 30 geregelt.
146 *Art. 29-Datenschutzgruppe*, WP 158, S. 13.
147 *Art. 29-Datenschutzgruppe*, WP 158, S. 12.

an den Erfordernissen der lex fori. Zu fordern ist, dass die Selektierung personenbezogener Daten begonnen wird, sobald eine Vereinbarung mit der gegnerischen Seite oder ein Gerichtsbeschluss über die Reichweite der Discovery vorliegt. Anonymisierung und Pseudonymisierung sind in der Regel noch nicht zwingend erforderlich.

1. Die Sicherung als Datenverwendung

Sobald vernünftigerweise mit einem Rechtsstreit vor einem US-Gericht zu rechnen ist oder er formell begonnen hat,[148] erfordern die Zivilprozessvorschriften sowohl des US-Bundesrechts als auch des Rechts einzelner US-Bundesstaaten, dass Informationen identifiziert, in der Regel ausgesondert und gesichert werden. Solche Informationen können personenbezogene Daten enthalten. Ist dies getan, existiert ein Bestand von „gesicherten Daten".

Nach der DS-RL und infolgedessen auch dem BDSG ist die bloße Sicherung personenbezogener Daten zu zivilprozessualen Zwecken – anders als aus US-amerikanischer Sicht – eine „Speicherung" und mithin als Datenverwendung einzustufen. Deshalb bedarf die Sicherung der gesonderten Erlaubnis,[149] da in den meisten Fällen die Daten nicht zum Zweck künftiger Gerichtsprozesse erhoben wurden. Gemäß den Grundsätzen der Datenvermeidung und Datensparsamkeit sind die personenbezogenen Daten zu löschen,[150] sobald sie nicht länger für den ursprünglichen nicht-prozessualen Verwendungszweck benötigt werden. Anders ist dies nur dann, wenn eine neue Erlaubnis die weitere Datenverwendung, vorliegend somit die fortdauernde Sicherung, zulässt.

2. Allgemeine Datenverwendungsvoraussetzung für die Sicherung: berechtigtes Interesse

Die Sicherung stellt eine Datenverwendung dar und erfordert daher entweder die Einwilligung oder eine spezifische gesetzliche Erlaubnis. In diesem Stadium ist Legitimierung mittels Einwilligung nicht zu verwirklichen, da die Daten nicht zu Prozesszwecken erhoben wurden, sodass eine ursprüngliche Einwilligung insoweit fehlt. Zudem wurden die Daten noch nicht detailliert ausgewertet, sodass in diesem Stadium die Betroffenen noch nicht einmal bestimmt sind. Damit ist von den – nicht identifizierten – Betroffenen eine Einwilligung schon aus praktischen Gründen kaum zu erlangen. Schließlich wird eine wirksame Einwilligung von Beschäftigten ohnehin in den seltensten Fällen zu erlangen sein.

Wie oben ausgeführt stellt die Verteidigung gegen eine Klage, unabhängig davon, ob sie in Deutschland oder einem anderen Land anhängig ist, ein berechtigtes Interesse der verantwortlichen Stelle dar. Die entscheidende Frage bei der datenschutzrechtlichen Bewertung ist, ob die Verhältnismäßigkeit i.S.d. für jeden Schritt der Datenverwendungskette erforderlichen Interessenabwägung bejaht werden kann. Die Abwägung der Rechte potenziell Betroffener und der berechtigten Interessen der verantwortlichen Stelle muss auf eine Lösung abzielen, die der verantwortlichen Stelle die Rechtsverfolgung erlaubt und gleichzeitig den Eingriff in die Interessen der Betroffenen minimiert.

a) Das Filtern personenbezogener Daten

Um den Interessen der Betroffenen das angemessene Gewicht i.R.d. Interessenabwägung zu verleihen, ist der genaue Umfang der involvierten Daten zu bestimmen.

Wenn personenbezogene Daten, die zulässigerweise erhoben wurden, zu Prozesszwecken gesichert werden, erscheint es zunächst als zulässig, potenziell prozesserhebliche Daten in einem verhältnismäßig großen Umfang aufzubewahren. In Übereinstimmung mit dem US-amerikanischen Discovery-Ansatz umfasst das auch Informationen, welche für sich genommen nicht erheblich sind, aber möglicherweise zur Aufdeckung relevanter Beweismittel führen. Obschon die Sicherung personenbezogener Daten, die sich bereits in der Sphäre der verantwortlichen Stelle befinden, sicherlich einen Eingriff in die Rechte des Betroffenen darstellt, da die Daten so über einen längeren Zeitraum existieren, ist der Eingriff eher als gering einzustufen. Dies gilt unbeschadet des Umstands, dass jede Datenverwendung das Risiko einer zufälligen oder strafbaren Preisgabe der Daten potenziell erhöht. Offensichtlich anerkennt auch das *BVerfG* grundsätzlich die Notwendigkeit eines gestaffelten Vorgehens. In einer Entscheidung zur behördlichen Beschlagnahmung von E-Mails hat es zunächst die Sicherung eines großzügigeren Umfangs von E-Mails zugelassen, da die sofortige Aussonderung der Nachrichten nicht durchführbar war. Allerdings verlangte es im Hinblick auf spätere dauerhafte und daher eingriffsintensivere Maßnahmen, dass die E-Mails so rasch wie möglich und zumutbar gefiltert werden.[151]

Ein strengerer Ansatz würde die Position der verantwortlichen Stelle erheblich und unverhältnismäßig beschneiden. Er könnte eine europäische Prozesspartei in einer US-Streitsache schon in der Sicherungsphase dazu zwingen, US-amerikanische Zivilprozessregeln, möglicherweise sogar Anordnungen des Gerichts zu verletzen und sich dadurch scharfen Sanktionen in den USA auszusetzen. Diese Konsequenz ginge zu weit, insbesondere gemessen an dem eher geringen Eingriff in die Rechte des Betroffenen. Da nur personenbezogene Daten gesichert werden dürfen, die von entsprechenden sich aus der lex fori ergebenden Verpflichtungen umfasst sind, erscheint es daher in diesem Stadium hinnehmbar, wenn die verantwortliche Stelle nicht dazu gezwungen wird, die personenbezogenen Daten schon bis auf die – im europäischen Verständnis dieses Begriffs – wirklich prozesserheblichen Informationen zu filtern.

Allerdings muss die verantwortliche Stelle sicherstellen, dass anfangs ausschließlich die Sicherung durchgeführt wird und dass die personenbezogenen Daten nicht anderweitig verwendet werden können. Außerdem sollte die logische oder sogar physische Trennung der maßgeblichen Daten von den allgemeinen Geschäftsdaten der verantwortlichen Stelle erwogen werden, um das Missbrauchsrisiko noch weiter zu reduzieren.

In Übereinstimmung mit den allgemeinen Grundsätzen unterliegt die verantwortliche Stelle der Pflicht, so rasch wie praktisch möglich und in jedem Stadium die angemessenen Schritte zu unternehmen, um den Umfang der gesicherten Daten zu begrenzen.[152] Sobald eine Verständigung mit der gegnerischen Partei oder ein entsprechender Beschluss des ausländischen Gerichts vorliegt, sind alle über das nötige Maß hinaus gesicherten personenbezogenen Daten zu löschen.

Der betreffende Filterungsprozess stellt ebenfalls eine Datenverwendung dar, namentlich in der Terminologie des BDSG eine „Nutzung" personenbezogener Daten gem. § 3 Abs. 5 BDSG. Da sie jedoch auf die Verringerung der gesicherten Datenmenge abzielt, ist diese Nutzung angesichts der allgemeinen Grundsätze der Datenvermeidung und Datensparsamkeit grundsätzlich positiv zu bewerten, da sie den Zwecken des Datenschutzes förderlich ist. Die Filterung ist daher grundsätzlich zulässig.

---

148 S. unter IV.2.c).
149 *Art. 29-Datenschutzgruppe*, WP 158, S. 8.
150 S. unter II.9.
151 *BVerfG* MMR 2009, 673, 678 m. Anm. *Krüger*.
152 Die *Art. 29-Datenschutzgruppe* scheint diesem Ansatz ebenfalls zu folgen, WP 158, S. 10.

b) Anonymisierung und Pseudonymisierung (noch) nicht erforderlich

In der Phase der Sicherung erscheint es im Licht des § 3a BDSG zulässig, die personenbezogenen Daten noch nicht zu anonymisieren oder pseudonymisieren. Während die Anonymisierung, die definitionsgemäß irreversibel ist, die verantwortliche Stelle denselben Gefahren aussetzen könnte wie die zu weit gehende Filterung zu diesem frühen Zeitpunkt, ist die (reversible) Pseudonymisierung gemessen an den Zwecken des Datenschutzrechts unverhältnismäßig, da sich die personenbezogenen Daten noch sicher in der Sphäre der verantwortlichen Stelle befinden. Für besonders gelagerte Einzelfälle mag eine andere Bewertung angezeigt sein, im Allgemeinen wird man jedoch nach der hier vertretenen Auffassung in dieser Phase, insbesondere mit Blick auf den damit verbundenen Aufwand, noch nicht die Anonymisierung oder Pseudonymisierung der Daten verlangen können.

c) Zeitliche Entstehung des berechtigten Interesses

Die Sicherungspflicht in den USA setzt spätestens in dem Moment ein, in dem ein Rechtsstreit unmittelbar bevorsteht, mit anderen Worten, wenn vernünftigerweise mit der Klageerhebung zu rechnen ist.[153] Um der verantwortlichen Stelle eine effektive Rechtsverteidigung in den USA zu ermöglichen, muss auch unter europäischem Datenschutzrecht zugelassen werden, dass zu diesem Zeitpunkt mit der Sicherung begonnen wird.

Allerdings genügt hierfür die bloße unsubstanziierte allgemeine Möglichkeit nicht, dass die verantwortliche Stelle eines Tages irgendeinem Rechtsstreit[154] ausgesetzt sein könnte.[155] Diese Auffassung steht nicht notwendigerweise im Widerspruch zu den US-amerikanischen Prozessvorschriften, da eine Prozesspartei gem. FRCP 37(e) keine Sanktionen durch ein US-Gericht zu befürchten hat, wenn die Löschung elektronisch gespeicherter Informationen sich „als das Ergebnis einer routinemäßigen, in gutem Glauben ausgeführten Bedienung eines elektronischen Informationssystems" darstellt. Alle routinemäßigen Löschungsvorgänge sind natürlich anzuhalten, sobald eine Sicherungspflicht nach US-Zivilprozessrecht besteht.

3. Gesicherte Daten: eine zusätzliche Sicherungskopie?

Nach US-amerikanischem Zivilprozessrecht dürfen keine erheblichen Daten mehr gelöscht werden, sobald eine Sicherungspflicht besteht. Andererseits sind bei Geltung des europäischen Datenschutzrechts sukzessive, immer weiter gehende Filterungsschritte zu verlangen. Für die verantwortliche Stelle besteht damit grundsätzlich die Gefahr, zwischen die Mühlsteine der Anforderungen der unterschiedlichen Rechtsordnungen zu geraten. Am Ende könnte ein US-Gericht gar die Entscheidung der verantwortlichen Stelle im Nachhinein in Frage stellen und die Offenlegung zusätzlicher Dokumente verlangen, die möglicherweise nicht mehr existieren, was für die verantwortliche Stelle schwerwiegende Sanktionen zur Folge haben könnte.

Vor diesem Hintergrund könnten verantwortliche Stellen versucht sein, eine vollständige Kopie der gesicherten Daten zu ziehen. Unter der Voraussetzung, dass der Zugriff auf eine solche Kopie nur im Falle eines entsprechenden US-Gerichtsbeschlusses möglich ist, kann mit Blick auf die praktischen Erfordernisse die Anfertigung einer solchen Sicherungskopie als Maßnahme, die den berechtigten Interessen der verantwortlichen Stelle dient und verhältnismäßig ist, mithin als datenschutzrechtlich zulässig angesehen werden. Soweit ersichtlich liegen zu dieser Frage allerdings keine Einschätzungen der Aufsichtsbehörden vor.

Es lässt sich vertreten, dass dieser Ansatz auch noch in Einklang mit der DS-GVO steht, trotz der ausdrücklich im Erwägungsgrund Nr. 30 und im Art. 5 (c) aufgestellten Beschränkungen. Allerdings sind größtmögliche Anstrengungen im Hinblick auf die Datensicherheit zu unternehmen. Zudem ist sicherzustellen, dass die Zugriffsmöglichkeit zu anderen Verwendungszwecken ausgeschlossen ist.

4. Spezifische Export-Anforderungen

Die Sicherung im oben dargestellten Sinne beinhaltet keinen Export personenbezogener Daten in die USA. Daher sind keine besonderen Export-Anforderungen zu erfüllen.

5. Datenschutzbeauftragter

Wie bereits oben dargestellt, sollte der Datenschutzbeauftragte möglichst schon in dieser Phase einbezogen werden.[156]

6. Beginn der Dokumentation

Sobald die ersten Schritte im Hinblick auf eine neue Datenverwendungskette vorhersehbar oder schon unternommen sind, sollte mit der Dokumentation dieser konkreten Datenverwendungskette begonnen werden. Im Idealfall beruht die Dokumentation auf den allgemeinen Datenschutzrichtlinien des Unternehmens und hält sie – natürlich – ein. Unternehmen, die transkontinentale Geschäftsaktivitäten betreiben und daher von transkontinentalen Rechtsstreitigkeiten betroffen sein können, sind gut beraten, solche RL aufzustellen. Diese allgemeinen RL sollten jedoch nur eine Grundstruktur vorgeben, da es schlimmer ist, die eigenen RL zu verletzen, als erst keine zu verabschieden.

V. Anwendung II: Interne Datenverwendung

Ein Rechtsstreit kann ohne Detailanalyse der gesicherten Daten nicht sinnvoll ausgetragen werden. Ab einem gewissen Zeitpunkt müssen diese Daten daher von der Prozesspartei weiter verarbeitet werden, um ihre berechtigten Interessen zu verfolgen. Nachfolgend wird unterstellt, dass die Interne Datenverwendung ohne einen Export personenbezogener Daten durchgeführt werden kann.

Die Interne Datenverwendung kann in der bereits oben erwähnten Form des Filterns erfolgen, nachdem die Reichweite der Discovery begrenzt wurde, oder in der des Sortierens und Analysierens, um die Tatsachen und die Hintergründe des Falls zu erforschen. Dies ist etwa für die Einschätzung des Falls und die Festlegung von Verteidigungsstrategien notwendig.

Die damit verbundene Datenverwendung kann – und wird üblicherweise – einerseits zu einer Verringerung, andererseits auch zu einer Vermehrung der personenbezogenen Daten führen. Erst durch die Prüfung und Analyse bestimmter Informationen werden weitere Informationsträger – Custodians – identifiziert mit der Folge, dass weitere Informationen zusammengetragen werden. Während die verantwortliche Stelle bei jedem Schritt die maßgeblichen Interessen im Einzelfall abwägen muss, sollte die resultierende notwendige Interne Datenverwendung im Allgemeinen keine zusätzlichen Probleme aufwerfen. Für die Sicherung dieser zusätzlichen Daten gelten keine über das oben Genannte hinausgehenden besonderen Anforderungen.[157]

---

153 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, S. 2.

154 *Brisch/Laue*, RDV 2010, 1, 3; *Spies/Schröder*, MMR 2008, 275, 278; *Art. 29-Datenschutzgruppe*, WP 114, S. 15; *Art. 29-Datenschutzgruppe*, WP 158, S. 8.

155 Die Frage, in welchem Umfang die Datenverwendung im normalen Geschäftsbetrieb zulässig ist, in diesem Fall zum Schutz gegen Ansprüche und Klagen im Allgemeinen, liegt außerhalb des Umfangs dieser Veröffentlichung.

156 S. unter III.9.

157 S. unter IV.

In Anbetracht des noch recht begrenzten Risikos für die Interessen der Betroffenen wäre es unverhältnismäßig, wenn man von der verantwortlichen Stelle verlangen würde, dass sie weitere Zeit und Geld raubenden Schritte in dieser Phase unternimmt. Es ist die klare Absicht des BDSG und des entsprechenden europäischen Gesetzgebungshintergrunds, der verantwortlichen Stelle zu erlauben, ihre Rechte vor Gericht zu verteidigen und sich dafür entsprechend zu rüsten. Jede Datenverwendung sollte jedoch ordnungsgemäß dokumentiert werden.

VI. Anwendung III: Externe Datenverwendung

Die Datenverwendung im Zusammenhang mit einem Rechtsstreit, der nicht in der Jurisdiktion der verantwortlichen Stelle, sondern in einem Staat außerhalb der EU, insbesondere in den USA, anhängig ist, hat diese Veröffentlichung motiviert. Sicherlich werden externe Übermittlungen im Endeffekt notwendig sein, um einen Rechtsstreit in den USA erfolgreich zu führen. Zum Zwecke dieses Kapitels wird davon ausgegangen, dass die Externe Datenverwendung, sei sie juristischer oder informationstechnischer Art, den Export personenbezogener Daten in die USA zur Folge hat.

Vom Blickwinkel der Verfolgung eines berechtigten Interesses i.S.d. § 28 BDSG aus betrachtet, macht es keinen Unterschied, ob die personenbezogenen Daten an einen externen Rechtsanwalt in der Jurisdiktion der verantwortlichen Stelle oder an einen Drittstaat, der möglicherweise einen weniger strengen Datenschutz gewährleistet, übermittelt werden. Allerdings erschwert es die Analyse wesentlich, wenn der Export an einen externen Rechtsanwalt in den USA erfolgt, da dann besondere Exportvoraussetzungen vorliegen müssen.

Die externe Datenverwendung der personenbezogenen Daten durch einen externen Rechtsanwalt, Dienstleistungsunternehmen und Experten ist auf der ersten, allgemeinen Prüfungsstufe insoweit zulässig, als sie zur Wahrung der berechtigten Interessen der verantwortlichen Stelle im Hinblick auf die Discovery und die Verteidigung gegen eine Klage vor Gericht erforderlich ist. In Bezug auf einen – auch US-amerikanischen – Rechtsstreit wird kaum eine vernünftige Datenverwendung innerhalb der EU je unverhältnismäßig sein; verantwortliche Stellen verfügen in der Regel nicht über die juristischen oder technischen Ressourcen, um die erforderliche Datenverwendung selbst durchzuführen.[158] Sobald jedoch ein Export notwendig ist, wird die Export-Abwägung im Allgemeinen nur dann zu Gunsten des Exports ausfallen, wenn jede durchführbare Filterung schon vorher vorgenommen wurde, die personenbezogenen Daten in der EU anonymisiert oder pseudonymisiert und die Betroffenen im nötigen Umfang ordnungsgemäß unterrichtet wurden.[159]

1. Allgemeine Datenverwendungsvoraussetzung für die externe Datenverwendung: Berechtigtes Interesse

§ 28 Abs. 2 Nr. 1 i.V.m. § 28 Abs. 1 Satz 1 Nr. 2 BDSG erlaubt die externe Datenverwendung personenbezogener Daten, soweit es zur Wahrung der eigenen Interessen der verantwortlichen Stelle erforderlich ist, mit anderen Worten, wenn es zur Verteidigung vor Gericht gegen eine Klage erforderlich ist. Es versteht sich von selbst, dass die gründliche Prüfung und Analyse der personenbezogenen Daten die Grundvoraussetzung dafür ist, dass der Prozessanwalt in den USA die verklagte verantwortliche Stelle zielführend verteidigen kann. Die externe Datenverwendung ist nicht nur deshalb zulässig, weil sie im Hinblick auf die Discovery, sondern allgemein für den Fall erforderlich ist. Deutsche wie US-amerikanische Rechtsanwälte können für die verantwortliche Stelle die gesicherten Daten im Großen und Ganzen sichten und prüfen, sofern sie nicht offenkundig übermäßige und irrelevante personenbezogene Daten enthalten oder die verantwortliche Stelle offensichtlich in der Lage ist, selbst die Informationen weitergehend zu filtern, zu anonymisieren oder zu pseudonymisieren, ohne dabei negative Konsequenzen befürchten zu müssen. Dies wird in Bezug auf Streitsachen in den USA so gut wie nie der Fall sein.

Die Einschaltung eines Dienstleistungsunternehmens ist ebenfalls zulässig.[160] Die verantwortliche Stelle wird fast nie imstande sein, die erforderlichen Vorbereitungshandlungen in informationstechnischer Hinsicht ohne externe Hilfe durchzuführen.

Aus diesem Grund ist die externe Datenverwendung, genau wie die Interne Datenverwendung, zulässig, da sie der Wahrung der berechtigten Interessen der verantwortlichen Stelle dient.[161]

2. Export-Abwägung im Detail

Darüber hinaus verlangt der Export personenbezogener Daten in die USA zusätzliche Sicherungsvorkehrungen, wie sich aus den §§ 4b und 4c BDSG ergibt. Die Messlatte ist dabei relativ hoch anzusetzen, da die USA gegenwärtig nicht als ein Staat anerkannt sind, der ein angemessenes Datenschutzniveau gewährleistet. Infolgedessen wird ein solcher Export generell missbilligt;[162] die Vermutung, die gegen den Export spricht, kann daher nur durch starke Sicherheitsmaßnahmen überwunden werden. Die drei Wege „sicherer Hafen", „Übermittlungsvertrag" und „Erforderlichkeit in Bezug auf Rechtsansprüche" können den Export nur legitimieren, sofern die exportbezogene Interessenabwägung entsprechend günstig ausfällt.[163] Dabei wird der Export in allen drei Szenarien grundsätzlich missbilligt und die Ausnahmen sind restriktiv anzuwenden, da es sich um die Übermittlung in ein Land ohne angemessenes Datenschutzniveau handelt. Daher neigt sich anfangs auch die Waagschale zu Ungunsten des Exports. Werden jedoch die folgenden Vorbedingungen erfüllt, kann die Übermittlung dennoch zulässig sein.

a) Filtern personenbezogener Daten vor der Übermittlung

Sobald der Export personenbezogener Daten erforderlich wird, muss der Umfang der personenbezogenen Daten, die vom Export unbedingt betroffen sind, beurteilt und reduziert werden. Mit anderen Worten, erst nachdem jeder machbare Schritt in Europa unternommen wurde, darf der verbleibende Rest exportiert werden. Der Betroffene, der in den meisten Fällen nichts getan hat, das es rechtfertigen würde, ihn einem US-Verfahren auszusetzen, hat ein berechtigtes Interesse daran, dass seine Daten weitestgehend aus einem Drittstaat herausgehalten werden. Der Prozess der Filterung der personenbezogenen Daten bis auf das absolute Minimum muss in der Regel in einem Staat durchgeführt werden, der ein angemessenes Datenschutzniveau gewährleistet.[164] Dieser ortsgebundene Vorgang ist im Allgemeinen unverzichtbar.[165] In einer Stellungnahme vom August 2009 teilt die *französische Datenschutzbehörde (CNIL)* diese Auffassung. Laut der *CNIL* müssen die Daten in

158 S. unter VI.1.
159 S. unter VI.2.
160 S. unter VI.2.
161 *Brisch/Laue*, RDV 2010, 1, 5; *Hanloser*, DuD 2008, 785, 787; *Spies/Schröder*, MMR 2008, 275, 278.
162 S. unter III.5.
163 S. unter III.6.
164 *Art. 29-Datenschutzgruppe*, WP 158, S. 11; *TSC*, for Analysis of Cross-Border Discovery Conflicts, S. 12.
165 *Brisch/Laue*, RDV 2010, 1, 7; es scheint, als ob *Spies* diese Auffassung teilt, vgl. MMR 7/2007, S. V, VII.

dem Land analysiert werden, in dem sie sich befinden.[166] Auch das *BayLDA* hat sich in diesem Sinne geäußert.[167]

Nur in seltenen und schwer zu rechtfertigenden Ausnahmefällen darf das Filtern zulässigerweise auch in einem Drittstaat, wie den USA, stattfinden; das kann im Wesentlichen dann der Fall sein, wenn die Forderung nach einer örtlichen Filterung unzumutbar ist.[168] Für den Fall, dass sich die verantwortliche Stelle für eine Filterung im Ausland entscheidet, ist eine ausführliche Dokumentation der Gründe dafür ebenso ratsam wie eine Zusammenarbeit mit der nationalen Aufsichtsbehörde. Die gegenteilige Auffassung, nach der nur der ausländische Rechtsanwalt die zu Grunde liegenden Einschätzungen ordnungsgemäß vornehmen könne, würde zu weit gehen und die berechtigten Interessen der einzelnen Betroffenen sowie das europäische Datenschutzsystem unzulässig außer Acht lassen.

b) Anonymisierung und Pseudonymisierung vor der Übermittlung

Angesichts der Missbilligung des Exports personenbezogener Daten in die USA durch die nationalen und europäischen Gesetzgeber ist zuzugeben, dass der Export das Risiko einer Schädigung der Interessen der Betroffenen exponenziell erhöht. Aus diesem Grund ist umso größeres Gewicht auf alle praktikablen Maßnahmen zum Schutz dieser Interessen zu legen. Eine der effektivsten Schutzmaßnahmen ist die Anonymisierung oder wenigstens die Pseudonymisierung der personenbezogenen Daten. In der Regel dürfen personenbezogene Daten erst übermittelt werden, nachdem sie anonymisiert oder pseudonymisiert worden sind, soweit es der Prozesszweck zulässt und solange die damit verbundene Anstrengung gegenüber dem gewünschten Schutz der Privatsphäre des Betroffenen nicht unverhältnismäßig ist. In den meisten Fällen wird es ausreichen, wenn die personenbezogenen Daten in einer pseudonymisierten Form mit individuellen Identifikationsmerkmalen, die vom Namen des Betroffenen unterschieden sind, übermittelt werden.[169] Die verantwortliche Stelle muss vor einer späteren Übermittlung zumindest verifiziert haben, ob eine solche Möglichkeit besteht.[170]

Falls die Besonderheiten des betreffenden Rechtsstreits die Übermittlung der personenbezogenen Daten in nicht einmal pseudonymisierter Form erfordern, ist eine detaillierte Dokumentation angezeigt.

c) Transparenz und Rechte auf Auskunft, Berichtigung und Widerspruch

Es ist fraglich, ob der Export personenbezogener Daten in die USA zusätzliche Transparenzmaßnahmen erfordert. Laut der *CNIL* sind die Betroffenen vor dem Export zu unterrichten über die Art der konkreten personenbezogenen Daten, die für die Datenverarbeitung verantwortliche Stelle, den Hintergrund des Verfahrens, den tatsächlichen Umstand, der die Offenlegung der Daten des Betroffenen erfordert, die Tatsache, ob die Offenlegung zwingend oder freigestellt ist, die Konsequenzen für den Betroffenen, falls er sich der Offenlegung widersetzt, und schließlich darüber, wie der Betroffene seine Rechte auf Auskunft, Berichtigung und Widerspruch in Bezug auf die Offenlegung der Informationen ausüben kann. Gemäß der *CNIL* darf der Betroffene nur dann nach erfolgter Übermittlung unterrichtet werden, wenn:

- die vorherige Unterrichtung die Beweisermittlung der verantwortlichen Stelle gefährdet, und
- eine vorläufige Regelung erforderlich ist, um die Vernichtung von Beweismitteln zu verhindern. Beide Ausnahmen sind in der Regel bei transkontinentalen Streitsachen nicht gegeben.

Während der Ansatz, der die Transparenz befürwortet, weitgehend auf Zustimmung trifft und demnach die Betroffenen unterrichtet werden sollten, ist ein Verhältnismäßigkeitstest zu implementieren. Nur die Maßnahmen, die vernünftigerweise von der verantwortlichen Stelle verlangt werden können, sind zwingend erforderlich.

VII. Anwendung IV: Offenlegung

Sobald es zur Offenlegung der Informationen vor Gericht kommt, können die verbliebenen personenbezogenen Daten unwiderruflich an die Öffentlichkeit gelangen, sofern nicht besondere Schutzmaßnahmen getroffen werden. Daher erfordert dieser letzte Schritt in der Datenverwendungskette die äußerste Sorgfalt und den weitestgehenden Schutz für den Betroffenen.

Aus diesem Grund sind die Filterung, die Anonymisierung oder Pseudonymisierung, die schon vor der Offenlegung durchzuführen sind, noch auszuweiten. Das ist insbesondere dann nötig, wenn – in seltenen Fällen – dies nicht schon vor der Externen Datenverwendung geschehen ist.[171] Darüber hinaus muss die verantwortliche Stelle grundsätzlich verbindliche Gerichtsbeschlüsse in Bezug auf die Discovery und geeignete Schutzanordnungen (protective orders) erlangen.[172]

1. Allgemeine Datenverwendungsvoraussetzungen für die Offenlegung vor Gericht

Letztlich wird die Offenlegung der personenbezogenen Daten gegenüber dem gegnerischen Lager (Rechtsanwälte und Sachverständige) sowie dem US-amerikanischen Gericht zu irgendeinem Zeitpunkt im Prozess unvermeidbar verlangt werden. Da § 28 Abs. 6 Nr. 3 BDSG sogar die Verwendung besonderer Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG erlaubt, um Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen, umfasst das berechtigte Interesse allgemein auch die Befolgung von Vorschriften des US-Zivilprozessrechts. Somit hat die verantwortliche Stelle grundsätzlich ein berechtigtes Interesse daran, personenbezogene Daten im erforderlichen Umfang offenzulegen.[173] Diesem Ansatz folgt auch die DS-GVO.[174] Allerdings ist auch klar, dass das Herausfiltern der personenbezogenen Daten auf das unbedingt erforderliche Minimum vor der Offenlegung vor Gericht die Grundvoraussetzung ist.

a) Filtern der personenbezogenen Daten vor der Offenlegung

Jede weiterführende Datenfilterung, die die verantwortliche Stelle keinen zusätzlichen Risiken im Hinblick auf US-amerikanische Streitsachen aussetzt, hat vor der Offenlegung zu erfolgen.

---

166 Délibération n°2009-474 du 23 juillet 2009 portant recommendation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dites de "Discovery."

167 *Bayerisches Landesamt für Datenschutzaufsicht* (*BayLDA*), Tätigkeitsbericht 2009/2010, S. 71, abrufbar unter: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht_2010.pdf.

168 *Brisch/Laue*, RDV 2010, 1, 5; *Hanloser* scheint zum selben Ergebnis zu kommen, DuD 2008, 758, 787. Sowohl *Brisch/Laue* als auch *Hanloser* verorten diese Thematik unter der Überschrift „Notwendigkeit" i.S.d. § 4c Abs. 1 Satz 1 Nr. 4 BDSG.

169 *Art. 29-Datenschutzgruppe*, WP 158, S. 11; die deutschen Aufsichtsbehörden teilen diese Auffassung; *Berliner Beauftragte für Datenschutz und Informationsfreiheit*, Jahresbericht 2006, S. 170, abrufbar unter: http://www.datenschutz-berlin.de/attachments/140/Jahresbericht_2006.pdf?1175508324; und Jahresbericht 2007, S. 191, abrufbar unter: http://www.datenschutz-berlin.de/attachments/438/Jahresbericht_2007.pdf?1207310269; *BayLDA*, Tätigkeitsbericht 2009/2010, S. 71, abrufbar unter: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht_2010.pdf.

170 *Brisch/Laue*, RDV 2010, 1, 6; *Spies/Schröder*, MMR 2008, 275, 280.

171 S. unter VI.

172 S. unter VII.1.c).

173 *Brisch/Laue*, RDV 2010, 1, 5; *Hanloser*, DuD 2008, 785, 787.

174 DS-GVO, Art. 9 lit. f.

b) Anonymisierung und Pseudonymisierung vor der Offenlegung

Falls personenbezogene Daten für eine Externe Datenverwendung ohne vorhergehende Anonymisierung oder Pseudonymisierung exportiert worden sind, ist mit äußerster Sorgfalt zu prüfen, ob solche Maßnahmen noch vor der Offenlegung vor Gericht ergriffen werden können.

c) Verbindliche Gerichtsbeschlüsse und Schutzanordnungen vor der Offenlegung

Außerdem ist vor der Offenlegung personenbezogener Daten an das betreffende US-Gericht heranzutreten. In dieser Hinsicht erklärt die *TSC* International Overview of Discovery, Data Privacy & Disclosure Requirements, dass Literatur und der *BfDI* einen verbindlichen Gerichtsbeschluss zur Offenlegung solcher Informationen und die Beschränkung der Reichweite der Discovery auf das fordern, was unbedingt erforderlich ist, um den Beschluss zu befolgen.[175]

Überdies könnten Parteien verpflichtet sein, Schutzanordnungen zu beantragen, um die Aufdeckung der übermittelten Informationen auf den Kreis der notwendigen Empfänger zu beschränken.[176] Daher ist es nötig, in jedem Einzelfall an das US-Gericht heranzutreten, die Datenschutzverpflichtungen, denen die verantwortliche Stelle unterworfen ist, darzulegen und entsprechende Schutzanordnungen zu beantragen, um die europäischen und nationalen Datenschutzvorschriften einzuhalten.[177] Die Prozessparteien in transkontinentalen Streitsachen sollten natürlich Vereinbarungen über diese Gegenstände treffen, bevor sie an das Gericht herantreten. *TSC* schlägt vor, dass die Parteien versuchen, sich auf adäquate Schutzanordnungen zu einigen. Diese können selbstverständlich noch einseitig beantragt werden, falls ein Einigungsversuch fehlschlägt.[178] Transkontinentale Discovery Mediation ist in dieser Hinsicht vielversprechend.

Wenn es allerdings einen klaren Hinweis darauf gibt, dass das betreffende Gericht im konkreten Einzelfall einem solchen Antrag nicht stattgeben wird, sollte die verantwortliche Stelle nicht auf das formelle Herantreten an das Gericht festgelegt werden, da dies dann eine bloße verzichtbare Formalie darstellen würde. Natürlich ist in einem solchen Fall eine angemessene Dokumentation angezeigt.

Von US-amerikanischen Gerichten sollte zu erwarten sein, dass sie angemessene Lösungen unterstützen, da der *US Supreme Court* im Aerospatiale-Fall hervorhob: „Amerikanische Gerichte, die vorgerichtliche Vorgänge überwachen, sollten besonders auf den Schutz ausländischer Parteien vor der Gefahr achten, dass sie durch unnötige – oder unangemessen belastende – Discovery in eine nachteilige Position manövriert werden."[179] Eine Schutzanordnung könnte die Versiegelung der Akte, die Beschränkung der Einsicht auf Rechtsanwälte („attorneys-eyes-only"), Einsicht nur im Zimmer des Richters („in camera") und zahlreiche weitere Optionen eröffnen.[180] Ein geeigneter Ansatz ist auf der Grundlage der konkreten Umstände des Einzelfalls auszuwählen.

Es ist allerdings festzuhalten, dass – um es vorsichtig auszudrücken – nicht alle US-Richter gleichermaßen gewillt sind, die Bedürfnisse ausländischer Beklagter in dieser Hinsicht anzuerkennen. Die Verbreitung der International Principles und ein wachsendes Bewusstsein hinsichtlich beider Rechtskulturen sollte allerdings die Zahl der Richter schrumpfen lassen, die sich der Problematik nicht bewusst sind.

Falls das US-Gericht nicht gewillt ist, die erforderlichen Schutzmaßnahmen zu erlassen, könnte dahingehend argumentiert werden, dass die Offenlegung vor Gericht überhaupt nicht zulässig ist. Die – grob gesagt – weitgefasste „Rechtsstreitausnahme" im Hinblick auf Streitsachen im Ausland könnte einen solchen Schluss erfordern. Denn grundsätzlich sind Schranken zu errichten, die gewährleisten, dass die personenbezogenen Daten nicht außerhalb eben dieses besonderen Verwendungszwecks verwendet werden können. Wenn das Gericht nicht bereit ist, zu dieser Sicherheit beizutragen, oder es von Beginn an deutlich wird, dass – aus anderen Gründen – die Datenempfänger den Zugriff auf die personenbezogenen Daten nicht auf den zulässigen Verwendungszweck begrenzen werden, müsste der Export untersagt werden. Falls die Öffentlichkeit Zugang zu den personenbezogenen Daten erhalten könnte, könnte die Position vertreten werden, dass die überwiegenden Interessen des Betroffenen die Datenübermittlung verbieten.[181] Allerdings sind im Kontext des Exports zum Zwecke transkontinentaler Gerichtsverfahren alle starren Regeln zu Gunsten einer Einzelfallanalyse zu vermeiden. Wenn die verantwortliche Stelle alle Schritte unternommen hat, die vernünftigerweise verlangt werden können, dann sind der Umfang und die Spezifika der personenbezogenen Daten sowie die Schutzmaßnahmen, zu deren Erlass das US-Gericht bereit ist, zu bewerten. Diese fallbezogenen Umstände liefern dann die Grundlage für die Entscheidung, ob der Export zu erlauben oder zu versagen ist.

VIII. Das Fernmeldegeheimnis am Arbeitsplatz

Das folgende Kapitel behandelt die besonderen Fragen, welche die Datenverwendung mit Blick auf das Fernmeldegeheimnis und die Frage seiner Geltung am Arbeitsplatz aufwirft. Insoweit besteht eine Reihe von Unsicherheiten, die ihre Ursache u.a. darin haben, dass neben dem Fernmeldegeheimnis als Grundrecht gem. Art. 10 Abs. 1 GG zusätzlich § 88 TKG auf einfachgesetzlicher Ebene das Fernmeldegeheimnis regelt. Gem. § 88 Abs. 1 TKG unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände (TK-Daten). § 88 TKG verpflichtet die Anbieter von TK-Dienstleistungen (Diensteanbieter) zur Wahrung des Fernmeldegeheimnisses.

Rechtsprechung und Literatur haben die genaue Reichweite des Fernmeldegeheimnisses am Arbeitsplatz und die sich daraus ergebenden Handlungsbeschränkungen für Arbeitgeber bislang noch nicht völlig eindeutig definiert. Selbst die Frage, ob das Fernmeldegeheimnis im Beschäftigungsverhältnis überhaupt gilt, ist nicht ganz zweifelsfrei geklärt. Die Autoren des vorliegenden Aufsatzes kommen jedenfalls zu folgenden Ergebnissen: Sofern der Arbeitgeber seinen Beschäftigten die Nutzung des Internet oder des E-Mail-Systems für private Zwecke ausdrücklich erlaubt oder diese zumindest duldet, ist er als Diensteanbieter anzusehen (vgl. unter VIII.1.). TK-Daten sind sowohl innerhalb als auch außerhalb von Beschäftigungsverhältnissen bis zum Abschluss der Datenübertragung vom Fernmeldegeheimnis geschützt. Die Datenübertragung endet erst, sobald der Kommunikationsteilnehmer die ausschließliche Kontrolle über Zugang, Vervielfältigung und Weiterleitung der Daten innehat. Unternehmen können nicht davon ausgehen, dass externe (d.h. nicht zu ihren Beschäftigten gehörende) TK-Teilnehmer mit Blick

175 *TSC*, International Overview 2009 – Deutschland, S. 103.
176 *TSC*, International Overview 2009 – Deutschland, S. 103.
177 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, S. 17; *Art. 29-Datenschutzgruppe*, WP 158, S. 11; *Spies/Schröder*, MMR 2008, 275, 280.
178 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, S. 17.
179 482 U.S. 522, 546 (No. 15, 16a).
180 *Rath/Klug*, K&R 2008, 596, 600; *Spies/Schröder*, MMR 2008, 275, 280.
181 *Spies/Schröder*, MMR 2008, 275, 279; für die gegenteilige wenig überzeugende Ansicht, wonach Art. 26 Abs. 1 lit. d der RL die meisten Problemkreise vorhergesehen und gelöst hat, *Hanloser*, DuD 2008, 785, 789.

auf das Fernmeldegeheimnis einen geringeren Schutzanspruch genießen (vgl. unter VIII.2.). Die unbefugte Verwendung von TK-Daten ist gem. § 88 Abs. 3 TKG untersagt und kann erhebliche Konsequenzen haben. Die wirksame Einwilligung aller betreffenden Kommunikationsteilnehmer kann zwar Eingriffe in das Fernmeldegeheimnis rechtfertigen; die Einwilligung ist jedoch in der Praxis nur schwer zu erlangen und kann nicht durch eine Einwilligung des Betriebsrats ersetzt werden. Sofern die Einwilligung aus tatsächlichen oder rechtlichen Gründen nicht eingeholt werden kann, muss der Arbeitgeber vom Beschäftigten verlangen, dass letzterer seine E-Mails sortiert und private E-Mails aus allen Speichermedien des Arbeitgebers entfernt. Es ist empfehlenswert, eine schriftliche Bestätigung des Arbeitnehmers hierüber einzuholen.

1. Der Arbeitgeber: Potenzieller Anbieter von TK-Diensten

Die Ausgangsfrage lautet, ob der Arbeitgeber Diensteanbieter ist. In der Fachdiskussion besteht dahingehend Einigkeit, dass der Arbeitgeber kein Diensteanbieter ist, wenn er den privaten Gebrauch des Internet und von E-Mail-Diensten ausdrücklich verbietet und auch nicht durch konkludentes Verhalten duldet.[182] In diesem Fall ist das TKG nicht anwendbar.[183]

Leider endet die Einigkeit bereits an dieser Stelle: Zwei Entscheidungen von Landesarbeitsgerichten aus jüngerer Zeit vertreten die Auffassung, dass der Arbeitgeber selbst dann kein Diensteanbieter sei, wenn er den Privatgebrauch zulässt.[184] Während einige Stimmen in der Literatur diese Ansicht teilen,[185] vertreten die h.M. und einige andere Gerichtsentscheidungen die gegenteilige Auffassung. Hiernach bietet der Arbeitgeber TK-Dienste „Dritten" i.S.d. § 3 Nr. 10 TKG an und ist deshalb als „Diensteanbieter" gem. § 3 Nr. 6 und Nr. 10 TKG zu qualifizieren.[186] Das wohl wichtigste Argument für diese Position besteht darin, dass § 3 Nr. 10 TKG für die Bejahung einer geschäftsmäßigen Erbringung von TK-Diensten weder eine Entgeltpflicht noch eine Gewinnerzielungsabsicht voraussetzt. Vielmehr genügt nach der Gesetzesbegründung insoweit jedes Erbringen von TK-Diensten.[187] Die deutschen Aufsichtsbehörden teilen weitestgehend – möglicherweise sogar einhellig – diese Auffassung.[188]

2. Das Ende der Datenübertragung

Soweit der Arbeitgeber als Diensteanbieter angesehen wird, besteht jedoch des Weiteren eine Reihe von Unsicherheiten hinsichtlich der Reichweite des Fernmeldegeheimnisses. Namentlich stellt sich die Frage, wann die Datenübertragung und damit der Schutz durch das Fernmeldegeheimnis enden. Zwar gibt es mehrere Entscheidungen des *BVerfG* zu dieser Frage; indessen bestreiten einige Autoren die Anwendbarkeit dieser Entscheidungen auf Beschäftigungsverhältnisse. Rechtsprechung, die sich ausdrücklich mit dem Fernmeldegeheimnis am Arbeitsplatz befasst, ist wiederum spärlich gesät und zudem uneinheitlich.

a) Überblick

Das *BVerfG* hat in einer Entscheidung aus dem Jahr 2009 den Schutzbereich des Fernmeldegeheimnisses als Grundrecht gem. Art. 10 Abs. 1 GG klargestellt.[189] Das *Gericht* bestätigte, dass sich das Fernmeldegeheimnis nicht auf gespeicherte Daten erstreckt, sobald die Datenübertragung beendet ist. In dieser Frage bestand indessen schon vorher Einigkeit in der juristischen Diskussion. Darüber hinaus hat das *Gericht* jedoch in dieser Entscheidung die Streitfrage geklärt, zu welchem Zeitpunkt die Datenübertragung bei der Telekommunikation per E-Mail endet.[190]

Da die Kommunikation mit einer nicht am selben Ort befindlichen Person die Mitwirkung eines Diensteanbieters erfordert und daher leichter dem – ggf. unbefugten – Zugriff Dritter ausgesetzt ist, lässt Art. 10 Abs. 1 GG solcher Kommunikation einen besonderen Schutz zukommen. Im Wesentlichen bezweckt Art. 10 Abs. 1 GG, den TK-Teilnehmern dasselbe Maß an Vertraulichkeit und Sicherheit zu bieten, das sie bei unmittelbarer Kommunikation – d.h. bei physischer Anwesenheit der Kommunikationspartner – genießen würden. Der Schutz erstreckt sich auf den Inhalt und die Umstände der Kommunikation und endet erst, wenn die Datenübertragung abgeschlossen ist. Informationen, die außerhalb der Datenübertragung gespeichert werden, sind nicht mehr von Art. 10 Abs. 1 GG geschützt. Der Nutzer ist jedoch nach dem Ende des Schutzes durch Art. 10 Abs. 1 GG nicht schutzlos gestellt, sondern genießt insoweit Schutz durch das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG.[191]

Hierbei ist das Ende der Datenübertragung anhand des Schutzes zu bestimmen, den das Grundrecht bezweckt, und nicht lediglich anhand technischer Umstände. Entscheidender Gesichtspunkt ist dabei die faktische Möglichkeit des Nutzers, den Zugriff, die Vervielfältigung und die Weiterleitung der E-Mail zu kontrollieren. Solange dem Nutzer die entsprechende Kontrollmöglichkeit fehlt, sind die Daten noch durch das Fernmeldegeheimnis geschützt; solange existieren mithin TK-Daten. Auch wenn frühere Entscheidungen des *BVerfG*, u.a. eine Entscheidung aus dem Jahr 2006,[192] möglicherweise eine davon abweichende Sicht angedeutet hatten, kommt es maßgeblich auf die tatsächliche Kontrollmöglichkeit des Nutzers in der konkreten Situation an. So ist es unerheblich, ob der Nutzer die E-Mail in einer Weise hätte speichern können, die ihm die ausschließliche Kontrolle ermöglicht hätte, wenn er dies tatsächlich im konkreten Fall nicht getan hat.[193] Wie selbst die Kritiker dieser Entscheidung einräumen müssen, hat das *BVerfG* in dieser grundsätzlichen Frage keinen Raum für Zweifel gelassen.[194]

In dem vom *BVerfG* entschiedenen Fall hatte ein Nutzer für den Zugriff auf seine E-Mails IMAP verwendet, und die E-Mails blieben auf dem Server des Diensteanbieters gespeichert. Da der

---

182 Die Entscheidung hinsichtlich der Privatnutzung steht im Ermessen des Arbeitgebers; *Altenburg/Reinersdorff/Leister*, MMR 2005, 135. Arbeitsverträge, Betriebsvereinbarungen und betriebliche Übungen können dieses Ergebnis jedoch modifizieren.

183 *Hoppe/Braun*, MMR 2010, 80 m.w.Nw.

184 *LAG Berlin-Brandenburg* ZD 2011, 43 m. Anm. *Tiedemann* = NZA-RR 2011, 342 ff.; *LAG Niedersachsen* NZA-RR 2010, 406 ff. = MMR 2010, 639 m. Anm. *Tiedemann*.

185 *Haussmann/Krets*, NZA 2005, 259, 261; *Wytibul*, ZD 2011, 69, 73.

186 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, S. 83; *Hoppe/Braun*, MMR 2010, 80, 81; *Altenburg/Reinersdorff/Leister*, MMR 2005, 135, 136; Anm. *Tiedemann*, ZD 2011, 45, 46; Taeger/Gabel/*Munz*, BDSG, § 88 TKG Rdnr. 20; Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, § 88 TKG Rdnr. 18; *Rath/Klug*, K&R 2008, 596, 598; *Hanloser*, DuD 2008, 785, 787, 788; *Härting*, Internetrecht, 4. Aufl. 2010, Rdnr. 130 f.; *Hoeren*, Onlineskript „Internetrecht", Stand: April 2011, S. 396, abrufbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/lehre/lehrematerialien.htm; *Polenz/Thomsen*, DuD 2010, 614; *Schmidl*, MMR 2005, 343, 344; Simitis/*Seifert*, BDSG, 7. Aufl. 2011, § 32 Rdnr. 92; *LAG Berlin-Brandenburg* ZD 2011, 43 m. Anm. *Tiedemann* = NZA-RR 2011, 342; *Brink*, in: jurisPR-Arbeitsrecht, Anmerkung zu *LAG Berlin-Brandenburg*; *OLG Karlsruhe* DuD 2005, 167 ff. = MMR 2005, 178 m. Anm. *Heidrich*; *ArbG Hannover* NZA-RR 2005, 420, 421.

187 BT-Drs. 13/3609, S. 53.

188 *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit* (*BfDI*), Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, Januar 2008, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenInternetAmArbeitsplatzneu.pdf?__blob=publicationFile.

189 *BVerfG* MMR 2009, 673 ff. m. Anm. *Krüger*.

190 Die verschiedenen Meinungen sind dargestellt von *Krüger*, MMR 2009, 680, 681.

191 *BVerfG* NJW 2006, 976, 978 = MMR 2006, 217.

192 *BVerfG* NJW 2006, 976, 978 = MMR 2006, 217.

193 *BVerfG* MMR 2009, 673, 674 m. Anm. *Krüger*.

194 Vgl. Anm. *Krüger*, MMR 2009, 680, 681.

Diensteanbieter somit noch Zugang zu den E-Mails hatte – und der Nutzer dementsprechend nicht über die ausschließliche Kontrollmöglichkeit hinsichtlich des Zugangs, der Vervielfältigung und Weiterleitung verfügte – war die Datenübertragung noch nicht beendet, sodass der Nutzer noch durch das Grundrecht des Fernmeldegeheimnisses geschützt war.[195] Keine Bedeutung kam nach Auffassung des *Gerichts* dem Umstand zu, dass der Nutzer seine E-Mails mit einem Passwortschutz versehen hatte und dass er keinen Gebrauch von der Möglichkeit gemacht hatte, die E-Mails vom Server zu löschen.

Einige weitere Aspekte, die das *BVerfG* berücksichtigt hat, stützen das Ergebnis, dass E-Mails, die auf dem Server des Diensteanbieters gespeichert sind, weiterhin TK-Daten darstellen, die somit dem Fernmeldegeheimnis unterliegen: Insbesondere ist der Diensteanbieter in dieser Situation noch in die Administration der E-Mail eingebunden.[196] Mangels ausschließlicher eigener Kontrollmöglichkeit kann der Nutzer den Zugang Dritter zu den TK-Daten nicht einseitig verhindern.[197] Die Gefahr eines heimlichen Zugriffs auf die TK-Daten besteht fort. Auch wenn diese Gefahr für das Eingreifen des Fernmeldegeheimnisses nicht konstitutiv ist, so ist sie doch zumindest typisch und erhöht das Gewicht möglicher Eingriffe in das Fernmeldegeheimnis.[198] Von einem übergeordneten Standpunkt aus betrachtet sind die TK-Daten nicht nur derselben Zugriffsmöglichkeit Dritter ausgeliefert, wie sie bei anderen Daten besteht, die ein Nutzer erstellt und gespeichert hat. Vielmehr besteht insoweit ein besonderes Risiko, das spezifisch aus der Übertragungssituation resultiert und gegen welches das Fernmeldegeheimnis Schutz bietet. Dieser Schutz gilt, solange eine E-Mail auf dem Server des Diensteanbieters gespeichert ist.

b) Sicht des Beschäftigten

Indessen gibt es unterschiedliche Ansichten zu der Frage, ob die oben angeführte Entscheidung des *BVerfG* auf Beschäftigungsverhältnisse überhaupt anwendbar ist. Auch wenn es seit diesem Urteil noch keine Gerichtsentscheidungen gab, die seine Anwendbarkeit auf Beschäftigungsverhältnisse ausdrücklich bestätigen, so wird die Anwendbarkeit in der Literatur doch mehrheitlich bejaht.[199] Die meisten dieser Autoren vertreten dabei die Ansicht, dass Arbeitsplatz-E-Mails vom Fernmeldegeheimnis als Grundrecht des Beschäftigten erfasst sind, wenn der Privatgebrauch des dienstlichen E-Mail-Accounts ausdrücklich erlaubt oder geduldet worden ist, und solange der Arbeitgeber eine Zugangsmöglichkeit zu den E-Mails hat, die vom Beschäftigten nicht ausgeschlossen werden kann. Dies soll nach Ansicht einiger Autoren auch dann gelten, wenn der Arbeitgeber nur über Backup-Speicherungen des E-Mail-Systems Zugriff auf diese E-Mails hat.[200] Sobald jedoch der Beschäftigte die E-Mails ausschließlich auf einen Speicherort außerhalb des E-Mail-Systems ablegt, selbst wenn die E-Mails dann für den Arbeitgeber noch zugänglich sind (z.B. wenn sie auf einem Unternehmensserver gespeichert sind), endet nach dieser – mehrheitlichen – Auffassung die Übertragung und damit auch der Schutz durch das Fernmeldegeheimnis.

Die Gegenansicht bestreitet die Anwendbarkeit der Entscheidung des *BVerfG* auf Beschäftigungsverhältnisse und begründet dies damit, dass die Entscheidung nur das Fernmeldegeheimnis i.S.d. GG betreffe, nicht hingegen das einfachgesetzlich geregelte Fernmeldegeheimnis gem. § 88 TKG. Die Vertreter dieser Ansicht argumentieren insoweit, dass Art. 10 Abs. 1 GG nur Behörden binde, nicht hingegen Unternehmen, für die demnach insoweit allein § 88 TKG maßgeblich sei. Das TKG jedoch – so diese Autoren weiter – erfasse nicht die ruhende Kommunikation,[201] da der Telekommunikationsbegriff des TKG gemäß der Definition in § 3 Nr. 22 TKG einen „dynamischen" Vorgang voraussetze.

Eine weitere, vermittelnde Ansicht bejaht zwar grundsätzlich die Anwendbarkeit des Fernmeldegeheimnisses auf Beschäftigte, jedoch ende dieser Schutz mit dem Senden oder Empfangen der einzelnen E-Mail, wenn es – abstrakt betrachtet – ausschließlich in der Macht des Arbeitnehmers steht, die E-Mail in dem E-Mail-System zu belassen oder sie von dort zu entfernen. Falls die E-Mail im E-Mail-System des Arbeitgebers belassen wird, obwohl für den Beschäftigten eine rechtmäßige Möglichkeit besteht, sie von dort zu entfernen, sei der Beschäftigte nicht mehr schutzbedürftig.[202]

Weder die ablehnende noch die vermittelnde Ansicht stehen vollständig im Einklang mit der o.g. Grundsatzentscheidung des *BVerfG* aus dem Jahr 2009. Der Schutz durch das Fernmeldegeheimnis ist erforderlich, solange die E-Mail auf dem Server des Diensteanbieters gespeichert ist und der Nutzer außerstande ist, einseitig den Zugriff des Diensteanbieters oder Dritter hierauf zu beschränken. Das *BVerfG* hat zudem der abstrakten Möglichkeit des Nutzers, die E-Mail vom E-Mail-Server zu entfernen, ausdrücklich keine Bedeutung zugemessen. Da die Entscheidung des *BVerfG* eine grundlegende Sicht des von Art. 10 Abs. 1 GG bezweckten Schutzes zum Ausdruck bringt, sprechen die besseren Argumente dafür, die einfachgesetzliche Vorschrift des § 88 TKG im Lichte des Grundrechts auszulegen und damit so, wie dieses vom *BVerfG* definiert wurde.[203]

Daher enden die Datenübertragung und damit der Schutz erst, sobald die E-Mail des Beschäftigten vollständig aus dem E-Mail-System des Arbeitgebers entfernt wurde und keine Wiederherstellungsmöglichkeit besteht.

c) Die Sicht Dritter

Noch komplexer wird die Lage, wenn auch Dritte in die Betrachtung miteinbezogen werden. Das Fernmeldegeheimnis schützt grundsätzlich alle an einem TK-Vorgang Beteiligten.[204] In Bezug auf die Kommunikation per E-Mail sind das der Absender und (alle) Empfänger. Bei E-Mail-Kommunikation eines Beschäftigten mit Außenstehenden – also Personen, die nicht zu den Beschäftigten dieses Arbeitgebers gehören – wäre damit sowohl die Einwilligung des Beschäftigten als auch die Einwilligung mindestens eines weiteren – nicht zu den Beschäftigten gehörenden – TK-Teilnehmers erforderlich.[205]

Nach Ansicht einiger Autoren endet der Schutz des Fernmeldegeheimnisses für den Absender, sobald die E-Mail auf dem Server des Empfängers bzw. seines Arbeitgebers eingegangen ist. Damit ist nach dieser Auffassung keine Einwilligung des drittbeteiligten Absenders einer E-Mail erforderlich.[206] Die Vertreter dieser Auffassung berufen sich auf eine Entscheidung des *BVerfG* aus dem Jahr 2006, gemäß der die Datenübertragung

195 *BVerfG* MMR 2009, 673, 675 m. Anm. *Krüger*.
196 *BVerfG* MMR 2009, 673, 675 m. Anm. *Krüger*.
197 *BVerfG* NJW 2006, 976, 978 = MMR 2006, 217.
198 *BVerfG* NJW 2006, 976, 978, 981; *BVerfG* MMR 2009, 673, 677 m. Anm. *Krüger*.
199 *Hoppe/Braun*, MMR 2010, 80, 82; in gleichem Sinne *Panzer-Heemeier*, DuD 2012, 48, 52; Anm. *Tiedemann*, ZD 2011, 45, 46.
200 *Hoppe/Braun*, MMR 2010, 80, 82; ebenso *de Wolf*, NZA 2010, 1206, 1209.
201 *Behling*, BB 2012, 892, 894; *Härting*, Internetrecht, Rdnr. 116, 140.
202 *Panzer-Heemeier*, DuD 2012, 48, 52; Anm. *Tiedemann*, ZD 2011, 45, 46; vermutlich auch Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, § 88 TKG Rdnr. 32; *VGH Kassel* NJW 2009, 2470 ff. = MMR 2009, 714.
203 Dies gilt, obwohl das *BVerfG* ausgeführt hat, dass der Umfang des Grundrechts den des in § 88 TKG verankerten Rechts übersteigen kann, *BVerfG* MMR 2009, 673 ff. m. Anm. *Krüger*.
204 BVerfGE 85, 386, 399; Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, § 88 TKG Rdnr. 14, 15; *Schmidl*, MMR 2005, 343, 346.
205 *Polenz/Thomsen*, DuD 2012, 614, 615.
206 *Kempermann*, ZD 2012, 12, 14; *Haussmann/Krets*, NZA 2005, 259, 261; in gleichem Sinne, aber in Hinblick auf Filterung von Spam-E-Mails *Sassenberg/Lammer*, DuD 2008, 461, 462.

endet, sobald die E-Mail empfangen wurde und die Möglichkeit besteht, die E-Mail aus dem E-Mail-System zu entfernen.[207] Sie argumentieren, dass ruhende Kommunikation „klassischerweise" nicht vom Fernmeldegeheimnis erfasst sei.[208] Da zudem der Absender einer E-Mail keine Kontrolle über deren Verwendung durch den Empfänger habe – weil letzterer die E-Mail löschen oder aber sie innerhalb oder außerhalb des E-Mail-Systems in einer Weise speichern könne, dass die E-Mail nicht mehr dem Fernmeldegeheimnis unterfiele –, habe er keinen Anspruch auf den Schutz durch das Fernmeldegeheimnis, sobald die E-Mail empfangen wurde. Ein weiteres Argument gegen die Schutzbedürftigkeit beruht auf dem Gedanken, dass jemand, der eine E-Mail an einen geschäftlichen E-Mail-Account sendet, in den meisten Fällen die beim Empfänger geltenden internen Regelungen zur Nutzung des geschäftlichen E-Mail-Accounts nicht kennt und dementsprechend keinen Schutz durch das Fernmeldegeheimnis erwarten darf.

Auch wenn diese Argumente eine gewisse Plausibilität für sich beanspruchen mögen, so ist es doch insgesamt schwer abzuschätzen, wie ein deutsches Gericht diese Frage in einem konkreten Rechtsstreit entscheiden würde. Auch sind in der Literatur tiefergehende Erörterungen hierzu kaum vorhanden. Hinzu kommt, dass die o.g. Entscheidung des *BVerfG* von 2009 für ein anderslautendes, weiter reichendes Verständnis des Fernmeldegeheimnisses spricht. So hat das *BVerfG* darin nicht etwa erklärt, dass die Ausweitung des Schutzbereichs des Fernmeldegeheimnisses auf ruhende Kommunikation nur auf den Empfänger beschränkt, der Absender hingegen hiervon ausgenommen wäre. Soweit TK-Daten in Rede stehen, sollten daher Unternehmen nicht davon ausgehen, dass insoweit die Einwilligung außenstehender Kommunikationsteilnehmer entbehrlich wäre.

3. Allgemeines Verbot der Verschaffung von TK-Daten

Soweit Daten dem Fernmeldegeheimnis unterfallen, untersagt § 88 Abs. 3 TKG dem Arbeitgeber, sich oder anderen über das für die geschäftsmäßige Erbringung der TK-Dienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus hiervon Kenntnis zu verschaffen. Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, dürfen nur für diesen in § 88 Abs. 3 TKG genannten Zweck verwendet werden. Informationen, die zum Zweck der Führung von geschäftsbezogenen Rechtsstreitigkeiten erhoben wurden, gehören ganz offenkundig nicht zu dieser Kategorie. Eine Verwendung dieser Daten für andere Zwecke, insbesondere die Weitergabe an Dritte, ist nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf TK-Vorgänge bezieht (§ 88 Abs. 3 Satz 3 TKG).

Betrachtet man die Gesetzesbegründung, wird das hohe Gewicht, das der Gesetzgeber dem Fernmeldegeheimnis zugemessen hat, weiter verdeutlicht. Förmliche Gesetze oder Eingriffsbefugnisse, auf Grund derer Behörden Auskünfte verlangen dürfen, vermögen Eingriffe in das Fernmeldegeheimnis nur zu rechtfertigen, wenn sich die entsprechende Befugnisnorm ausdrücklich auf TK-Vorgänge bezieht und aus ihr der Wille des Gesetzgebers deutlich wird, das Fernmeldegeheimnis insoweit zurücktreten zu lassen. Hingegen vermögen Rechtsvorschriften, die lediglich allgemeine Auskunftsverpflichtungen begründen, ohne ausdrücklich auf TK-Vorgänge Bezug zu nehmen und ohne diesen gesetzgeberischen Willen erkennen zu lassen, Eingriffe in das Fernmeldegeheimnis nicht zu rechtfertigen.[209]

So regelt etwa § 93 Abgabenordnung (AO) die Befugnis der Finanzbehörden, von Dritten die zur Feststellung eines für die Besteuerung eines Kunden erheblichen Sachverhalts erforderlichen Auskünfte zu verlangen. Jedoch können Finanzbehörden unter Berufung auf diese Vorschrift von einem Finanzinstitut keine Auskunft zu TK-Daten verlangen, die dem Fernmeldegeheimnis unterfallen, da § 93 AO nicht ausdrücklich auf TK-Vorgänge Bezug nimmt. *Hoppe/Braun* nennen hierzu einen Fall, bei dem die *US-Börsenaufsichtsbehörde* (*SEC*) involviert war: auf Grund eines Ersuchens der *SEC* in einer Insiderhandel-Angelegenheit forderte die *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)* von einem Unternehmen die Herausgabe von E-Mails, die von bestimmten Beschäftigten gesendet bzw. empfangen worden waren. Die für das Ersuchen angeführte gesetzliche Rechtsgrundlage – § 7 Abs. 7 i.V.m. § 4 Abs. 3 Wertpapierhandelsgesetz (WpHG) – regelt jedoch nur, dass die nationale Behörde bestimmte Informationen und Dokumente von jedermann verlangen kann. Da diese Rechtsgrundlage für das Auskunftsersuchen nicht konkret auf TK-Vorgänge Bezug nimmt, könnte das Unternehmen dem behördlichen Auskunftsersuchen nur unter Verstoß gegen das TKG nachkommen.[210]

Keine der derzeit geltenden Vorschriften des deutschen oder europäischen Rechts, die als Rechtsgrundlage für die Erhebung oder Nutzung von Daten für Zwecke der Führung allgemeiner geschäftsbezogener Rechtsstreitigkeiten in den USA in Betracht kommen, erfüllt die dargestellten Anforderungen an die Erhebung oder Nutzung von TK-Daten, die dem Fernmeldegeheimnis unterfallen. Weder die Befolgung zivilprozessualer Regeln eines ausländischen Staats noch der Beschluss eines ausländischen Gerichts vermögen den Eingriff in das Fernmeldegeheimnis zu rechtfertigen. Rechtfertigungsgründe, die zumindest nach einer vertretenen Auffassung Eingriffe in das Fernmeldegeheimnis zur Abwendung von Schäden, z.B. bei Verdacht auf Straftaten oder auf Verrat von Geschäftsgeheimnissen, u.U. legitimieren können,[211] sind in diesem Zusammenhang nicht einschlägig.[212]

Nimmt man nach alledem an, dass das Fernmeldegeheimnis für den Fall der erlaubten oder geduldeten E-Mail-Nutzung für private Zwecke auch am Arbeitsplatz gilt und sich zudem auch auf „ruhende Kommunikation" erstreckt, so kann der Arbeitgeber hiervon umfasste TK-Daten in Ermangelung entsprechender Einwilligungen nicht überwachen oder kontrollieren. Selbst das Screening solcher E-Mails, z.B. mittels Schlüsselwortsuchanfragen, verstößt dann bereits gegen § 88 Abs. 3 TKG.[213]

Sofern private E-Mails nicht eindeutig von den geschäftlichen E-Mails zu trennen sind, müssen die Geschäfts-E-Mails wie private behandelt werden. Somit „infizieren" die privaten E-Mails gewissermaßen die Geschäfts-E-Mails. Denn dem Arbeitgeber kann nicht erlaubt werden, in einem ersten Schritt sämtliche E-Mails zu untersuchen oder zu sortieren mit dem Argument, dass er anschließend nur die Geschäfts-E-Mails näher untersuchen wird. Vielmehr muss die Unterscheidung zwischen privaten und geschäftlichen E-Mails richtigerweise vor jedem Schritt der Datenverwendungskette getroffen werden. Selbst die Kennzeichnung einzelner E-Mails als „privat" durch den Beschäftigten löst das Problem nicht, da eingehende E-Mails in den meisten Fällen dem Erfordernis einer solchen Kennzeichnung nicht entsprechen werden.[214]

---

207 *BVerfG* NJW 2006, 976 ff. = MMR 2006, 217; nachfolgend *VGH Kassel* NJW 2009, 2470 ff. = MMR 2009, 714.
208 *Kempermann*, ZD 2012, 12, 14.
209 BT-Drs. 13/3609, S. 53 in Hinblick auf die (identische) Vorgängervorschrift § 82 Abs. 3 TKG.
210 *Hoppe/Braun*, MMR 2010, 80, 83.
211 *Hoppe/Braun,* MMR 2010, 80, 81, tragen vor, dass eine solche Ausnahme überwiegend unterstellt wird, was zwar den widerstreitenden Interessen gerecht wird, aber nicht im Einklang mit dem Wortlaut des Gesetzes steht.
212 *Hanloser*, DuD 2008, 785, 787 f. m.w.Nw.
213 *Hoppe/Braun*, MMR 2010, 80, 81; *Hanloser*, DuD 2008, 785, 787.
214 *Hoppe/Braun*, MMR 2010, 80, 83; *Koch*, NZA 2008, 911, 913; *Vietmeyer/Beyers*, MMR 2010, 807, 809.

4. Folgen der Verletzung des Fernmeldegeheimnisses

Zumindest jede unerlaubte Weiterleitung von Daten, die dem Fernmeldegeheimnis unterliegen, an Dritte stellt eine strafbare Handlung gem. § 206 Abs. 1 StGB dar. Das Verbot solcher Übermittlungen betrifft gleichermaßen den Diensteanbieter als solchen wie auch seine Beschäftigten.

Im Falle der Übermittlung von TK-Daten besteht somit ein tatsächliches Strafbarkeitsrisiko, wenn keine Einwilligung vorliegt.[215] Dies gilt selbst für Übermittlungen an den externen Unternehmensanwalt in Deutschland, Europa oder in Übersee, daneben freilich auch für Übermittlungen an den Anwalt der Gegenseite, an Dritte und an das US-Gericht. Selbst wenn entsprechende Daten lediglich anderen Beschäftigten des Diensteanbieters überlassen werden, wie z.B. Syndici oder internen Experten, ist eine Strafbarkeit nicht ausgeschlossen, da nach dem Gesetzeswortlaut jede unbefugte Mitteilung an eine andere Person und damit auch an einen anderen Beschäftigten strafbar ist.[216]

Keine Anwendung findet § 206 StGB, wenn TK-Daten lediglich unrechtmäßig erlangt wurden, ohne dass jedoch eine Weiterleitung an Dritte erfolgt wäre. Allerdings werden die geschützten Daten in den meisten Fällen personenbezogene Daten im oben definierten Sinne[217] darstellen, sodass hierin eine unbefugte Erhebung personenbezogener Daten und damit eine Ordnungswidrigkeit liegen kann,[218] die mit einer Geldbuße bis zu € 300.000,– geahndet werden kann.[219]

5. Wirksame Einwilligung

In Anbetracht dieser schwerwiegenden Konsequenzen, speziell der Strafbarkeitsrisiken, die eine Verletzung des Fernmeldegeheimnisses nach § 88 Abs. 3 TKG nach sich ziehen kann, sind Unternehmen gut beraten, davon auszugehen, dass TK-Daten nicht ohne Einwilligung der betroffenen Personen in die USA übermittelt werden dürfen.[220] Dies steht auch im Einklang mit der Feststellung der *TSC*, wonach ein Bereich „privater" Kommunikation (private E-Mails) existiere, der durch das Gesetz, insbesondere durch § 88 TKG, geschützt sei. In den Worten der *TSC*: „Diese ‚private Kommunikation' würde wahrscheinlich nicht der Discovery unterliegen", solange keine Einwilligung vorliegt.[221]

a) Einwilligung der betreffenden TK-Teilnehmer

Angesichts dieses erheblichen Risikos sind Arbeitgeber bemüht, Möglichkeiten zur Legitimierung des Umgangs mit Daten, die dem Fernmeldegeheimnis unterliegen, zu finden. Soweit eine wirksame Einwilligung vorliegt, scheidet eine Strafbarkeit nach § 206 Abs. 1 StGB aus, da es dann am Tatbestandsmerkmal der „Unbefugtheit" fehlt.

Soweit die Einwilligung der betreffenden TK-Teilnehmer erforderlich ist,[222] ordnet das Gesetz dafür keine besondere Form an. Somit kann eine Einwilligungsklausel in den Arbeitsvertrag aufgenommen werden. Auch eine gesonderte Einwilligungserklärung des Beschäftigten, die mündlich oder sogar konkludent ergehen kann, genügt insoweit.[223] Durch Betriebsvereinbarung kann bestimmt werden, dass der Privatgebrauch nur erlaubt ist, wenn eine wirksame Einwilligung des einzelnen Arbeitnehmers vorliegt, und dass eine entsprechende Einwilligung konkludent durch die Nutzung des Internet oder des E-Mail-Systems zu privaten Zwecken abgegeben wird.

Die Einwilligung kann jedoch nur dann als wirksam angesehen werden, wenn der Beschäftigte durch entsprechende Information in die Lage versetzt wurde,[224] die Reichweite seiner Einwilligung zutreffend zu erfassen.[225] Die ordnungsgemäße Information des Arbeitnehmers setzt voraus, dass der Beschäftigte eindeutig darüber aufgeklärt wurde, dass aus Gründen der Befolgung von Verpflichtungen zur Offenlegung von Daten, die sich aus dem US-amerikanischen Discovery-Recht ergeben, Eingriffe in sein Fernmeldegeheimnis in Betracht kommen. Zusätzlich wird vorgeschlagen, dass die Information darlegt, dass insoweit alle Arten elektronisch gespeicherter Daten betroffen sein können, und dass die potenziellen Empfänger der TK-Daten – interne und externe Rechtsanwälte und Experten, Dienstleistungsunternehmen, Prozessparteien, US-Gerichte – genannt werden.

Wenn es an jeglicher Art von Einwilligung fehlt, muss der Arbeitgeber – als letztes Mittel – vom Beschäftigten verlangen, dass dieser seine E-Mails durchsieht und alle privaten E-Mails entfernt, bevor der Arbeitgeber die Daten weiter verwendet.[226]

b) Einbeziehung des Betriebsrats

TSC vertritt die Auffassung, dass sowohl der Einzelne als auch der Betriebsrat des Unternehmens eine Einwilligung erklären und damit die Datenverwendung autorisieren könne.[227] Diese Aussage ist zumindest irreführend: Selbst wenn man nur die Einwilligung des Beschäftigten verlangen würde – nicht also auch die Einwilligung des Kommunikationspartners, der außerhalb des Unternehmens des Beschäftigten steht –, kann die Einwilligung des Betriebsrats nicht die Einwilligung des einzelnen Beschäftigten ersetzen. Denn anders als § 4 Abs. 1 BDSG enthält das TKG keine Öffnungsklausel,[228] auf Grund derer Eingriffe in das Fernmeldegeheimnis des einzelnen Beschäftigten durch Tarifverträge oder Betriebsvereinbarungen möglich wären. Aus diesem Grund vermögen solche kollektiven Regelungen für sich gesehen keine Eingriffe in das Fernmeldegeheimnis zu rechtfertigen.

Soweit eine Unternehmensrichtlinie zum Umgang mit TK-Daten am Arbeitsplatz verabschiedet werden soll und ein Betriebsrat existiert, muss indessen der Betriebsrat beteiligt werden. Dieser hat gem. § 87 Abs. 1 Nr. 6 BetrVG weitgehende Mitbestimmungsrechte im Hinblick auf die Einführung und die Nutzung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.[229] Daher schlagen einige Autoren – unbeschadet des Erfordernisses individueller Einwilligungen der Beschäftigten – vor, eine Bestimmung in die betreffende Betriebsvereinbarung aufzunehmen, wonach unter bestimmten, näher definierten Voraussetzungen Eingriffe in das Fernmeldegeheimnis erfolgen können.[230]

---

215 Eine weitergehende detaillierte Analyse etwaiger Rechtfertigungen liegt außerhalb des Umfangs dieser Veröffentlichung.

216 Hierauf kann i.R.d. Veröffentlichung nicht näher eingegangen werden.

217 S. unter I.

218 § 43 Abs. 2 Nr. 1 BDSG. Der Inhalt der E-Mail stellt weder Bestandsdaten noch Verkehrsdaten i.S.d. § 3 Nr. 3 und 30 TKG dar. Deshalb greifen nicht die Datenschutznormen des TKG (§§ 91 ff. TKG), sondern die des BDSG ein.

219 § 43 Abs. 3 BDSG.

220 *Rath/Klug*, K&R 2008, 596, 598 f.

221 *TSC*, International Overview 2009 – Deutschland, S. 100.

222 Zur Frage, welche Einwilligungen notwendig sind, s. unter VIII.2.

223 Aus Beweisgründen wird eine formlose Einwilligung jedoch nicht empfohlen.

224 *Gola/Wronka*, Hdb. zum Arbeitnehmerdatenschutz, 5. Aufl. 2010, Rdnr. 1827.

225 Eine schriftliche Bestätigung darüber, dass die entsprechenden Informationen erhalten wurden, ist aus Beweisgründen empfohlen. 1. TB der Bayerischen Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich (Regierung von Mittelfranken) 2002/2003, S. 54, abrufbar unter: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht2002-2003.pdf.

226 *Hanloser*, DuD 2008, 785, 788.

227 *TSC*, International Overview 2009 – Deutschland, S. 100.

228 *Altenburg/Reinersdorff/Leister*, MMR 2005, 222, 223; *Haussmann/Krets*, NZA 2005, 259, 263; *Hoeren*, Onlineskript „Internetrecht", Stand: April 2011, S. 396, abrufbar unter: http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/lehre/lehrematerialien.htm.

229 Simitis/*Seifert*, BDSG, 7. Aufl. 2011, § 32 Rdnr. 94; *Rath/Klug*, K&R 2008, 596, 599; *Spies*, MMR 7/2007, S. V, VII; *Haussmann/Krets*, NZA 2005, 259; *Däubler*, Gläserne Belegschaften, 5. Aufl. 2010, Rdnr. 833.

230 *Pröpper/Römermann*, MMR 2008, 514, 517; *Polenz/Thomsen*, DuD 2010, 614, 616; *Haussmann/Krets*, NZA 2005, 259, 261.

IX. Ergebnis

Zweifellos besteht ein Spannungsverhältnis zwischen den US-Zivilprozessvorschriften, insbesondere denjenigen zur konventionellen und elektronischen Discovery, und dem Datenschutz in der EU und Deutschland. Die DS-GVO wird den Konflikt nicht abmildern (vgl. unter I und II).

Das BDSG lässt die Verwendung personenbezogener Daten nur zu, wenn diese durch das BDSG selbst oder andere deutsche oder europäische Gesetze erlaubt wird oder wenn der Betroffene im Vorhinein wirksam eingewilligt hat. Jeder Schritt in der Datenverwendungskette muss dabei einzeln beurteilt werden und erfordert eine entsprechende Erlaubnis. Alle allgemeinen und besonderen Voraussetzungen, welche zur Datenverwendung berechtigen, unterliegen den Leitprinzipien der Datenvermeidung und Datensparsamkeit (vgl. unter II).

Der Export personenbezogener Daten in transkontinentalen Rechtsstreitigkeiten erfordert eine zweistufige Prüfung, da die wirksame Einwilligung aller Betroffenen – aus tatsächlichen oder rechtlichen Gründen – kaum jemals zu erlangen sein wird. Insoweit müssen sowohl die allgemeinen gesetzlichen Voraussetzungen der Verwendung personenbezogener Daten als auch zusätzliche exportbezogene Anforderungen erfüllt werden. Die Wahrung der berechtigten Interessen der verantwortlichen Stelle bildet die allgemeine Rechtsgrundlage – mithin die Rechtsgrundlage auf der ersten Stufe der Datenverwendung – gem. § 28 BDSG, wohingegen die „Notwendigkeit in Bezug auf Rechtsansprüche" die exportspezifische Rechtsgrundlage gem. §§ 4b und 4c BDSG bietet.

Eine Interessenabwägung ist schon auf der ersten Stufe erforderlich, um die Verhältnismäßigkeit zu gewährleisten; eine exportbezogene Interessenabwägung ist zusätzlich durchzuführen, um die Übermittlung personenbezogener Daten in ein Drittland, den Export, rechtfertigen zu können. Was die Export-Abwägung betrifft, so neigt sich die Waagschale in der Ausgangslage zu Ungunsten des Exports, da der Export allgemein nicht befürwortet wird (vgl. unter III.).

Unter Anwendung der Prinzipien und Grundregeln (vgl. unter III.) wurde ein Leitfaden im Hinblick auf jeden einzelnen Schritt in der Datenverwendungskette entwickelt:

Die Sicherung der Daten einschließlich der Erstellung einer Back-up-Kopie ist in dem Maße zulässig, wie es die lex fori erfordert (vgl. unter IV.). In der Phase der Internen Datenverwendung bestehen keine allgemeinen zusätzlichen Anforderungen (vgl. unter V.).

Rechtsstreitigkeiten innerhalb oder außerhalb der EU erfordern zumeist eine aufwändige Externe Datenverwendung – auch personenbezogener Daten – durch externe Anwälte, Dienstleistungsunternehmen und externe Experten. Auf der allgemeinen Prüfungsstufe wird die damit verbundene Datenverwendung wohl meist als zulässig anzusehen sein, da sie im Hinblick auf eine angemessene Verteidigung gegen eine Klage vor Gericht erforderlich ist (vgl. unter VI.1.). Vor dem Export personenbezogener Daten müssen jedoch alle zumutbaren Filterungen durchgeführt, die personenbezogenen Daten anonymisiert oder pseudonymisiert und die Betroffenen ordnungsgemäß in angemessenem Umfang unterrichtet werden (vgl. unter VI.2.).

Die Offenlegung personenbezogener Daten darf erst erfolgen, nachdem die abschließende Filterung, Anonymisierung und Pseudonymisierung mit äußerster Sorgfalt vorgenommen worden sind. Außerdem sind angemessene Gerichtsbeschlüsse bzgl. der Discovery und bzgl. des Datenschutzes zu erwirken, zumindest zu beantragen (vgl. unter VII.).

Hinsichtlich des TK-Rechts am Arbeitsplatz wurde festgestellt, dass der Arbeitgeber Diensteanbieter ist, wenn er den Privatgebrauch des Internet oder des E-Mail-Systems erlaubt oder duldet. Sobald der Arbeitgeber als Diensteanbieter angesehen wird, unterliegen die betroffenen TK-Daten dem Schutz des Fernmeldegeheimnisses bis zum Abschluss der Datenübertragung. Die Datenübertragung ist – innerhalb wie außerhalb von Arbeitsverhältnissen – erst abgeschlossen, sobald der TK-Teilnehmer die ausschließliche Kontrolle über die Daten erlangt hat. Die unbefugte Verwendung von Daten, die dem Fernmeldegeheimnis unterliegen, setzt den Diensteanbieter und seine Beschäftigten schwerwiegenden Konsequenzen aus. Die wirksame Einwilligung aller betreffenden TK-Teilnehmer kann zur Datenverwendung berechtigen; sie ist in der Praxis jedoch nur schwer zu erlangen. Eine Einwilligung kollektivrechtlicher Art vermag die Datenverwendung nicht zu legitimieren. Soweit die Einwilligung aus tatsächlichen oder rechtlichen Gründen nicht eingeholt werden kann, muss der Beschäftigte die Geschäfts- von den Privat-E-Mails trennen. (vgl. unter IV.4.), bevor der Arbeitgeber auf die geschäftlichen E-Mails zugreifen kann.

Dr. Ralf Deutlmoser
ist Rechtsanwalt und Mediator in München. Er ist in Deutschland und den USA (New York) als Rechtsanwalt zugelassen.

Alexander Filip
ist Leiter des Referats Internationaler Datenverkehr, Industrie, Handel, Gewerbe, Dienstleistungen beim Bayerischen Landesamt für Datenschutzaufsicht (Ansbach). Der vorliegende Beitrag gibt ausschließlich seine persönliche Auffassung wieder.

Content

ZEITSCHRIFT FÜR DATENSCHUTZ
SUPPLEMENT

RALF DEUTLMOSER / ALEXANDER FILIP

European Data Privacy versus U.S. (e-)Discovery Obligations

A Practical Guide For Enterprises

Transcontinental Litigation
Transparency
Specific Export Requirements
Anonymization
Data Protection Offices

■ The conflict between European Data Privacy laws and U.S. (e-)discovery obligations is currently almost unmanageable for German and European enterprises. Provided that the Sedona Conference was correct in its December 2011 statement, whereby the subject is „an area often thought of as so complex and confounding that it has been largely ignored", the relevant enterprises run a tremendous risk. The penalties are severe and a directed verdict in the US litigation could be the ultimate consequence of non-compliance.
This guide for enterprises will provide a practically usable and comprehensive approach to manage the respective conflict. It takes into account the publications of the Article 29 Working Party, of the Sedona Conference, and the January 2012 draft EU regulation.
It will be demonstrated that each and every handling of personal data requires a specific permission. Safeguarding the data controller's legitimate interests can provide such permission on a general level and the necessity with respect to foreign legal claims on the export-specific level. Besides the general balancing test, an export-specific additional balancing test has to be performed, with respect to which the scale initially tips on the side of non-transfer. Generally, the export is legitimate only after all reasonable culling, anonymization or pseudonymization, and information of the data subjects is done.
Finally, telecommunication privacy at the workplace is examined. Provided that the employer explicitly allows for or tolerates private use of the Internet or e-mail services, it has to be considered a provider of telecommunication services. As a consequence, the telecommunication information is protected by the right to telecommunication privacy until the conclusion of the data transmission. This conclusion occurs only once the participant gains exclusive control over the data.

■ Der Konflikt zwischen U.S.-amerikanischen prozessualen Offenlegungspflichten im Rahmen der (e-)Discovery und deutschem bzw. europäischem Datenschutzrecht ist derzeit kaum beherrschbar. Trifft die Aussage der Sedona Konferenz aus dem Dezember 2011 zu, wonach das Thema so komplex und verwirrend ist, dass es weitgehend ignoriert wird, gehen die betroffenen Unternehmen ein ganz erhebliches Risiko ein. Die Strafen sind empfindlich und die möglichen Folgen in den amerikanischen Zivilverfahren reichen bis hin zum sofortigen Unterliegen im Prozess.
Diese Sonderbeilage zeigt einen Weg auf, den Konflikt praktisch handhabbar zu machen und berücksichtigt dabei die Veröffentlichungen der Art. 29-Datenschutzgruppe, der Sedona Konferenz und den Entwurf der EU-Datenschutz-Verordnung (DS-GVO) aus dem Januar 2012.
Es wird aufgezeigt, dass jede Verwendung personenbezogener Daten der gesonderten Erlaubnis bedarf. Der Schutz berechtigter Interessen der verantwortlichen Stelle kann auf der allgemeinen datenschutzrechtlichen Prüfungsebene, die Erforderlichkeit der Verwendung in Bezug auf Rechtsansprüche vor einem ausländischen Gericht auf der exportspezifischen Prüfungsebene zu einer solchen Erlaubnis führen. Neben der „normalen" Interessenabwägung ist jedoch eine exportspezifische Abwägung durchzuführen, hinsichtlich derer die Waagschale zunächst zu Ungunsten des Exports geneigt ist. Im Regelfall ist der Export nur zulässig, nachdem alle zumutbaren Filterungen durchgeführt wurden, nach der Anonymisierung oder Pseudonymisierung und nach ordnungsgemäßer Unterrichtung der Betroffenen.
Abschließend wird das Telekommunikationsrecht am Arbeitsplatz betrachtet. Sofern der Arbeitgeber den Privatgebrauch von Internet oder E-Mail-System explizit erlaubt oder duldet, ist er als Diensteanbieter anzusehen. Die Telekommunikationsdaten unterliegen dann dem besonderen Schutz des Fernmeldegeheimnisses. Dieser endet mit dem Abschluss der Datenübertragung, der dann eintritt, wenn der Telekommunikationsteilnehmer die ausschließliche Kontrolle über die Daten erlangt.

I. The Entrepreneur – „Servant of Two Masters"

European entrepreneurs and enterprises involved in litigation in the U.S. are constantly trying to serve two masters:[1] European data privacy laws and U.S. rules of civil procedure, more specifically (e-)discovery obligations. Not surprisingly, this attempt poses significant difficulties, as „[...] conflicts arise between data protection law and other fundamental rights and legal requirements (e.g. e-discovery [...]) which puts businesses in the position of not knowing which law to comply with."[2]

Both sides of the Atlantic recognize the resulting dilemma as well as the potential harm to global trade: While it is recognized that cross-border data flows are necessary for the expansion of international trade,[3] the complexity of the rules on international transfer of personal data is considered as constituting a substantial impediment to the operations of economic stakeholders.[4] The dilemma has reached such a magnitude, that in February of 2012, the *American Bar Association* opined that the current practice of court rulings in the U.S., which may be seen „parochial or insufficiently accommodating of interests and mores of other legal regimes, could stymie the growth of global commerce".[5]

In addition, the problem is multiplied by differing implementations and interpretations of the current EU directive – starting with such core principles as the definition of personal data – by the legislators and relevant authorities in the Member States.[6] In the event the step on the European level from the current EU directive to a future regulation will be made as currently proposed, such differences on a national level will decrease significantly.

The relevant issues not only require a clarification of the European and national laws,[7] but rather a „new-deal approach" as the current EU legislative framework pre-dates the mega-trend of global data transfers.[8] It remains to be seen whether the „Consultation on the legal framework for the fundamental right to protection of personal data" initiated in July 2009 by the *European Commission*, which will likely lead to a European data privacy regulation, will provide a precise and manageable framework. This is especially crucial as the penalties and administrative sanctions set forth in the current draft are enormous and amount to up to 2% of the data controller's annual worldwide turnover.[9] Unfortunately, the current draft does not indicate such an approach and is far from a „Copernican Revolution";[10] at least with respect to the issues discussed in this publication, despite its declaration that „legal and practical certainty should be reinforced."[11] At this stage it seems that one of the biggest challenges to be addressed by a future regulation, the topic of transfer of personal data to countries outside of the EU,[12] will not be sufficiently addressed.

Unfortunately, despite the practical relevance for enterprises and even the world's economy, parties to litigation are on very unstable grounds,[13] and it is difficult to provide precise guidance with respect to the effects of data privacy laws on (e-)discovery demands.[14] Even worse, according to *The Sedona Conference („TSC")*, this area of law is „often thought of as so complex and confounding that it has been largely ignored."[15] Summing up, all stakeholders are dissatisfied with the current rules.[16]

While it is true since biblical times that „no one can serve two masters; for either he will hate the one and love the other, or else he will be loyal to the one and despise the other",[17] this publication provides a practical guide enabling enterprises to deal with the risks posed by the prescribed issues appropriately and avoid the choice between „God and mammon",[18] or at least between EU data privacy and U.S. (e-)discovery obligations. It will provide a bilingual outline of the subject to be used on both sides of the Atlantic and therewith enable the parties, authorities, and courts to demonstrate „due respect to the data protection laws of any foreign sovereign" as requested by Principle 1 of *TSC's* International Principles on Discovery, Disclosure and Data Protection („TSC International Principles").[19]

Unfortunately, there are no „quick-and-dirty solutions", but after laying the ground (Chapter II), the analysis of the requirements for handling personal data for transcontinental litigation purposes in general (Chapter III) leads to an outline, along which a generalized case can be dealt with. Obviously, a case-by-case adaptation is required, but at least a basis for a strategic approach with respect to each step of the handling chain, which is defensible in the U.S. as well as in Germany, is established (Chapters IV – VII). Finally, several issues with respect to telecommunications law at the workplace and the restrictions placed on employers' conduct are dealt with in the event they allow or tolerate private use of the Internet (Chapter VIII).

The results of the analysis can be summed up with the phrase: Balancing is the name of the game.

II. Background and Guiding Principles

While U.S. discovery obligations and EU data privacy and other laws are undoubtedly at odds, the conflict can only be understood properly and ways to overcome the differences be developed, if one takes the basic differences in litigation culture as well as the different concepts of data privacy into account. Prior to a detailed analysis, the background of the conflict as well as the underlying guiding principles of data privacy laws have to be examined.

1. Concept of Pre-Trial Discovery

The main reason for the conflict discussed in this publication is the U.S. concept of pre-trial electronic and conventional discovery. By and large, discovery – as for example set forth in the U.S. Federal Rules of Civil Procedure – is the formal procedure according to which litigants and third parties to litigation have to provide and may obtain information relevant for a dispute. The main purposes of discovery are to uncover as many facts as possible, to level the playing field of litigation with respect to any information imbalance, and, in general, to enable the litigants to better understand the facts of a dispute and the evidence introduced at trial.[20]

---

1 „Arlecchino servitore di due padroni" was written by *Carlo Goldoni* in 1745.
2 *ICC*, Response to the European Commission Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data dated December 2009, p. 3.
3 GDPR(p2012), Whereas 78.
4 Memorandum(2012), p. 4.
5 *American Bar Association*, Section of International Law, Resolution 103, Report to the House of Delegates, p. 2.
6 Described, e.g., in: *AmCham EU*, Response to the Commission Consultation on Protection of Personal Data, p. 4 f.
7 *Spies/Schröder*, MMR 2008, 275, 281.
8 *AmCham EU*, Response to the Commission Consultation on Protection of Personal Data, p. 2.
9 GDPR(p2012), Article 78, 79.
10 *Kuner*, 11 PVLR 06, 14.
11 Memorandum(2012), p. 2.
12 *Kuner*, 11 PVLR 06, 9.
13 *Spies*, MMR 7/2007, p. V, VI.
14 *Hoppe/Braun*, MMR 2010, 80, 84.
15 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. VI.
16 *Kuner*, 11 PVLR 06, 9.
17 *Matthew*, 6, 24.
18 *Matthew*, 6, 24.
19 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 7.
20 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 1.

To ensure comprehensive discovery, a corresponding obligation exists in the U.S. to preserve information relevant to litigation, once it has commenced or is to be reasonably anticipated.[21] Such information has to be secured and cannot – within or outside of a regular document retention process – be discarded. From a practical perspective, litigants in the U.S. send out „litigation hold letters" to (potential) custodians of relevant information. Through those letters, the custodians learn about pending or reasonably anticipated litigation in detail and are instructed to secure the information described.

Due to the importance placed on discovery, a joint understanding should be reached early in litigation between the parties. To foster this aim, Rule 26f of the U.S. Federal Rules of Civil Procedure requires litigants to „meet and confer" early in the process to discuss the relevant issues and reach agreements.

As strange as it may seem from a European perspective, even – and especially – information is covered that is harmful to the party bearing the burden of preservation and disclosure: the proverbial „smoking gun" has to be handed over to the opponent. From an U.S. perspective, the preservation and disclosure obligation is a cornerstone of litigation and a fundamental step in the administration of justice.

Most civil law countries take quite a contrary approach. In principle it is up to each party to discover the facts supporting its case and to offer the required evidence. Should a party require and desire to rely upon evidence in the hands of the other party, it has to identify such evidence in general.[22] By and large, civil law systems do not support „fishing expeditions",[23] pre-trial discovery is not a known concept and disclosure obligations are rare or practically non-existing in civil litigation.

Therefore, litigants in the U.S. – but not in Europe – are under high pressure to identify and produce (electronic or conventional) documents and materials that (potentially) relate to litigation. Such documents will in almost all instances contain personal data relating to employees, suppliers, customers or other third parties. If the personal data is covered by European data privacy legislation – to be more exact, at least currently, by national implementation laws of the Member States –, conflicts can arise between the preservation and disclosure obligations and the respective data privacy law.

2. Data Privacy – A Constitutional Right

Not only the differences in the rules of civil procedure provide a basis for the clash of legal cultures, but also the importance placed on data privacy in general. In 1983 the *German Federal Constitutional Court* held that Article 2 para. 1 Grundgesetz (German Constitution, „GG") in connection with Article 1 para. 1 GG contains a basic right to informational self-determination („informationelle Selbstbestimmung"). It contains the guarantee that each individual can decide about the disclosure and use of its personal data itself. This basic right can only be infringed upon if justified by an overwhelming public interest and if allowed for by a provisio contained in a formal law.[24] In addition to the basic right contained in the German Constitution, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms as well as Article 16 para. 1 of the Treaty on the Functioning of the European Union (TFEU) contain similar rights. However, it needs to be noted, that data privacy is not an absolute right, as underlined by the *European Court of Justice*.[25]

Without elaborating further on this issue, it can be assumed, that the abuse of governmental powers preceding and during World War II by Nazi Germany and its allies on the one hand and by communist regimes especially during the Cold War on the other hand is one of the main reasons for the importance placed on data privacy in Europe. Massive data collection efforts by the authorities, even if driven by matters of national security, are criticized heavily even today.[26] The historic roots as well as the current political discussions and developments should be kept in mind when evaluating the differences between the European and the U.S. approach to data privacy and when commenting on either body of law.

Communication with and understanding of the opposite legal culture is complicated by the fact that not even the technical terms are used accordantly. In this publication, „data privacy" is used instead of the prevalent translation of „data protection" for „Datenschutz", unless the technical protection of data, in the sense of „data security" / „Datensicherheit", is discussed.

3. Legal Basis of European and German Data Privacy Laws

On an European level, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the „Directive") is currently the relevant legislative act.[27] The Federal Data Protection Act (Bundesdatenschutzgesetz, „BDSG") transforms not only the Directive but implements the guiding principles set forth by the *German Constitutional Court* as discussed above.[28]

Consultations initiated by the *European Commission* in July 2009 led to the „Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" („GDPR(p2012)"), which was officially issued on 25 January 2012. Apart from the GDPR(p2012) the proposal consists of an explanatory memorandum regarding the proposed regulation („Memorandum(2012)"), and a proposed directive „on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data". Due to a lengthy and complex EU legislative process and a proposed two-year transition period, a regulation will likely not take effect before 2015, 2016 or even 2017.[29] Relevant Articles of GDPR(p2012) will be discussed in this publication where those provide insights into the current understanding of the law on a European level or an outlook on what to expect from a future regulation.

It remains to be seen, if a final regulation will initiate a „Copernican"-like „revolution" shifting the focus away from „paper-based, bureaucratic requirements" towards „compliance in practice", harmonization, and individual empowerment.[30] At least with respect to the issues discussed here, this seems unlikely and it is stated with respect to the GDPR(p2012) that it „some-

21 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 2.

22 According to Section 142 para. 1 sentence 1 Zivilprozessordnung (German Code of Civil Procedure, „ZPO"), a court can require the production of a document referred to by a party. This section does not allow for „fishing expeditions" as a specific document has at least to be identifiable. The mere assertion that like documents usually exist within the sphere of the opponent or a third party in a given situation is insufficient; *Musielak*, ZPO, 8. Edition 2011, Section 142 ZPO, marginal 4.

23 *Working Party*, WP 158, p. 4; *Hanloser*, DuD 2008, 785.

24 BVerfGE 65, 1, 43.

25 Memorandum(2012), p. 6 with further references.

26 *Künast*, ZRP 2008, 201, 203.

27 Official Journal L 281, 23/11/1995, 0031 – 0050.

28 See Chapter II.2.

29 Serious doubts exist, if the GDPR(p2012) violates the German Constitution. A detailed analysis of this issue lies outside of the scope of this publication.

30 *Kuner*, 11 PVLR 06, 1.

times loses sight of the need to adopt provisions that can actually be implemented in practice, and to be precise and meticulous in drafting."[31]

4. „Personal Data"

The BDSG covers „Personal Data" only. In line with the intention of the European lawmaker,[32] Section 3 para. 1 BDSG defines the term broadly as any information concerning the personal or material circumstances of an identified or identifiable natural person (the „data subject").

Personal Data covers any information concerning personal or material circumstances, which can be any sort of objective or subjective statement about a person regardless of position or capacity of this person and irrespective of the format (e.g., alphabetic, numerical, graphical, photographical or acoustic); may it be kept on paper, computer memory or audio/video tape.[33] An express or implied statement about attendance at a certain meeting or a record of making a certain statement suffices.[34] Most e-mails meet this criterion as they contain, e.g., the e-mail addresses of the sender and the recipient, the corporate function of the sender, and a statement of the sender (content of the e-mail).

The information has to relate to an identified or identifiable individual. This is the case, if it is about the individual or facts that relate to the individual.[35] More specifically, if it refers to the identity, characteristics, or behavior of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated.[36]

In the area of corporate information, the data subject can reside within the company, its supplier or customer base or it can be any other natural third party.

As the concept of Personal Data covers not only private but also professional matters, most corporate e-mails contain Personal Data.[37] In other words, practically every single corporate e-mail has to be considered Personal Data under European and national law.[38]

5. „Sensitive Personal Data"

A subset of Personal Data is considered so sensitive that special safeguards are put in place by the Directive and the German implementation law. „Sensitive Personal Data" contains explicit or context-based information[39] about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life (Section 3 para. 9 BDSG). In the event the Handling of Sensitive Personal Data requires special attention, the required safeguards are set forth in the respective chapter.

6. Territorial Scope of the BDSG

The BDSG is applicable, if Personal Data is collected, handled or used in Germany. Handling occurs in Germany, if the physical process is conducted in Germany (especially if the server or computer is located in Germany).[40] With respect to collection and use of Private Data it is sufficient that either the data is located in Germany or the data controller operates in Germany.[41]

The GDPR(p2012) will not confine the territorial scope from a practical perspective. Article 3 para. 1 GDPR(p2012) states that it applies to the Handling of Personal Data in the context of the activities of an establishment of a controller in the Union.

7. Addressee of the BDSG

While the Directive binds only the Member States and leaves to the national authorities the choice of form and method in accordance with Art. 288 TFEU, the BDSG as the German implementation act binds not only national authorities[42] but also private bodies unless the data is collected or handled solely for personal or domestic matters.[43]

8. Permission Based Handling

The paramount principle of German data privacy is set forth in Section 4 para. 1 BDSG, according to which any and all kind of collection, procession, and use (jointly: „Handling") of personal data shall be lawful only, if permitted or ordered by the BDSG or other law, or if the data subject has provided consent. The BDSG postulates a statutory ban with reservation on the granting of permission („Verbotsgesetz mit Erlaubnisvorbehalt") within its rather broad scope.[44]

Every step and every purpose of a given Handling chain, in this case the litigation chain, has to be evaluated separately. In the event the purposes of the Handling changes, the legality has to be re-evaluated based on the new purpose. In other words, legal Handling for one purpose does not implicate legality if Handling is done in relation to a new or further purpose.

In this context, „collection" (Section 3 para. 3 BDSG) means the acquisition of data, while „processing" entails, according to Section 3 para. 4 BDSG:

- Recording: entry, recording or preservation of personal data;
- Alteration: modification of the substance of recorded personal data;
- Transfer: disclosure of personal data to a third party either through transfer of the data to a third party or by the third party inspecting or retrieving data available for inspection or retrieval.

On a side note, the „French Blocking Statute [...] prohibits requesting, seeking, or disclosing in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings."[45]

9. Data Reduction and Data Economy

Other cornerstones of German and European data privacy law are data reduction and data economy as set forth in Section 3a sentence 1 BDSG. The right to informational self-determination

---

31 *Kuner*, 11 PVLR 06, 14.
32 *Working Party*, WP 136, p. 4.
33 *Working Party*, WP 136, p. 6 f.
34 The *Working Party* sets forth that, e.g., the prescription of a physician to an anonymous patient contains Personal Data about the prescriber; *Working Party*, WP 136, p. 7.
35 Däubler/*Weichert*, BDSG Kompaktkommentar, 3. Edition 2010, Section 3, marginal 19.
36 *Working Party*, WP 136, p. 9; *Working Party*, WP 105, p. 8; according to the *Working Party*, three elements can alternatively be used to determine if such relation exists: content element (information is given about a person), purpose element (information will be used to treat a person in a certain way), or result element (it is likely that the information has an impact on the rights and interests of a person), *Working Party*, WP 136, p. 10 f.
37 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, 181 f.
38 *FIOS*, Webcast 09-04-21: E-Mail in U.S. is "Personal Data" in EU and elsewhere; *TSC*, Framework for Analysis of Cross-Border Discovery Conflicts, p. 9.
39 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 3, marginal 65.
40 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, p. 176 f.
41 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, p. 177 f.
42 Däubler/*Weichert*, BDSG Kompaktkommentar, 3. Edition 2010, Section 1, marginal 9.
43 Private data collection and Handling is covered only if the private body collects data for use in data processing systems, or uses such systems to process or use data, or collects data in or from non-automated filing systems; Section 1 para. 2 sentence 3 BDSG.
44 Däubler/*Weichert*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4, marginal 1.
45 *TSC*, Framework for Analysis of Cross-Border Discovery Conflicts, p. 21.

is the basis from which the requirements for data reduction and data economy follow.[46] In essence, as little Personal Data as possible shall be collected, handled and used. Whenever several equally effective concepts are available for a specific task, the one requiring the least amount of Handling of Personal Data has to be chosen.[47]

In its principles relating to the processing of Personal Data, GDPR(p2012), Article 5 (c) states that Personal Data has to be „adequate, [and] relevant, limited to the minimum necessary in relation to the purpose for which they are processed".

As the permission to handle Personal Data is purpose-based and follows a necessity requirement, the data shall be rendered anonymous or pseudonymous as allowed for by the purpose for which it is collected and further handled as long as the required effort is not disproportionate to the desired purpose of privacy (Section 3a sentence 2 BDSG). In addition, once the purpose for the Handling is met, the respective Personal Data has to be deleted.[48] In other words, a deletion step builds the end of each Handling chain and has to be incorporated in its design.

The GDPR(p2012) sets forth the concept of data reduction even more explicit than the Directive.[49] Accordingly, the Personal Data handled shall not be excessive and the period of storage kept to a „strict minimum".[50]

Another consequence of those general axioms set forth in Section 3a sentence 1 BDSG is that the scope of the Personal Data has to be evaluated constantly and culled down to the extent reasonably possible.

Handling of Personal Data for litigation purposes can only be legitimate, if it is relevant for the specific litigation. The notion of relevancy, however, is quite different in the U.S. compared to the German legal system. According to the U.S. approach, information which is only likely to lead to the discovery of relevant evidence is already discoverable and needs to be preserved, whereas the European privacy laws would suggest an approach of „direct and objective relevance". A decision for one concept over the other should not be made in the abstract but rather in the context of each step in the Handling chain.

III. Handling of Personal Data for Transcontinental Litigation – Principles and Basic Rules

After laying the general foundation, the focus now shifts to the particularities of Handling Personal Data for transcontinental litigation. The guiding rules and principles will be defined in this chapter, before the results will be practicably applied to each step of the Handling chain.

This chapter will show the following: As valid consent of all relevant data subjects will – for practical and legal reasons – hardly ever be obtained,[51] Handling of Personal Data for transcontinental litigation purposes requires a two-step evaluation: general Handling requirements have to be met as well as Export specific additional requirements. While Personal Data may generally be handled to safeguard the controller's legitimate interest, in this case the defense against a legal claim, provided a Balancing Test shows that the Handling is proportional,[52] the Export requires that a specific Export Balancing Test is met as well. This test, with the scale initially tipping on the side of non-Export, is required irrespective if the legal basis for the Export is a Safe Harbor Scheme, a Transfer Contract, or „necessity related to legal claims".[53] Enterprises are well advised to involve the DPO as soon as reasonably possible, to keep the data subjects informed to the extent adequate and to establish data protection mechanisms in line with the risk posed. Naturally, proper documentation on all steps based on the enterprise's general and data privacy policy is good practice.[54]

1. The Handling Chain with Respect to Transcontinental Litigation

It was already stated that the Handling of Personal Data requires permission on each step of the Handling chain. For the sake of simplicity, the following four-step scheme is used hereafter: Initially, information potentially containing Personal Data has to be identified and securely stored. It needs to be ensured, that any regular or irregular process of deletion is stopped („Preservation"). Once Preservation has occurred, the data is reviewed internally („Internal Review"), before external counsels and experts review the information („External Review"). Eventually, the information will have to be handed over to the other party or the U.S. court („Production"). Transfer of Personal Data to a third country, „Export", will occur before or during external review, at the latest at the time of Production.

2. Consent: Unlikely to be a Practical Option

Consent of the data subject would be the preferable and (conceptually) easiest form of legitimization of Handling the Personal Data. Unfortunately, it seems unlikely that valid consent can be obtained in the context of (most cases of) U.S. litigation.[55] In line with this understanding the *Working Party* concluded in 2005 already: „Relying on consent may therefore prove to be a 'false good solution', simple at first glance but in reality complex and cumbersome."[56] This negative assessment is based on factual as well as legal reasons.

Practically, the general requirements for valid consent are – especially in cases where the scope of Preservation and Handling extends to hundreds of thousands or millions of documents or files – almost impossible to meet. According to Section 4a para. 1 BDSG consent is effective only, if each individual data subject was properly informed about the purpose of the Preservation or any later Handling prior to it. Proper information not only requires setting forth the scope and the purpose of the Preservation but, at least in later stages, also of the potential recipients of the Personal Data.[57] A carte blanche – e.g., in the employment contract or a separate declaration sent to all employees – that would allow for the Handling of all Personal Data for all purposes does not qualify as valid consent.[58]

While at this point in time it might theoretically be possible to include a specific clause in the individual employment contract covering Handling for litigation purposes, it is assumed that most employment contracts do not include such a clause currently. In addition, it would be quite difficult to use a precise enough clause to obtain valid informed consent for all kinds of litigation in advance. Naturally, such consent would not cover non-employees such as suppliers, customers or other third parties.

46 BVerfGE 65, 1, 43.
47 *Conrad*, CR 2005, 537.
48 *Brisch/Laue*, RDV 2010, 1, 3; *Spies/Schröder*, MMR 2008, 275, 278.
49 *Kunert*, 11 PVLR 06, 5.
50 GDPR(p2012), Whereas 30.
51 See Chapter III.2.
52 See Chapter III.4.
53 See Chapter III.5.
54 See Parts III.9 through III.13.
55 *Spies*, MMR 7/2007, p. V, VII.
56 *Working Party*, WP 114, p. 11.
57 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4b, marginal 8.
58 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, p. 79; *Working Party*, WP 114, p. 12.

Neither can consent be obtained collectively, especially via union contracts („Betriebsvereinbarung").[59] Hence, consent has to be given individually and with respect to the actual purpose – foreign litigation. Therefore, in litigation encompassing massive volumes of Personal Data, obtaining the required consent does not seem to be a practical solution. In addition, it needs to be noted, that the consent can be freely withdrawn for any or no reason without any negative consequences for the employee.

In the event Sensitive Personal Data is handled, the consent has to explicitly cover those. It is argued that the Sensitive Personal Data has to be incorporated into the wording of the consent itself.[60]

The consent shall be given in writing (excluding e-mail), unless special circumstances warrant a different form.[61] The consent has to be given prior to the Handling, later consent does not rectify the violation of the statute.[62]

The main legal reason, however, why it is unlikely that valid consent can be obtained is that it has to be given freely. The data subject has to have a real opportunity to withhold or withdraw its consent without having to fear negative consequences as a result of the decision.[63] In the event that the data subject is an employee of the controller, it is at least highly advisable to set forth explicitly that the employee will not be subject to negative consequences should he not consent or withdraw his consent at a later point in time.[64]

It has to be noted that some authors argue that an employee can (almost) never validly consent because of the nature of the employment relationship;[65] it seems to be the more convincing approach to argue that a rebuttable presumption against voluntariness exists.[66] From a practical perspective, the data controller is at least on very unstable grounds if it relies on consent of an employee. It is therefore not recommended to make use of consent, unless no other option exists.

The GDPR(p2012) tightens the requirements even further as it will be valid only, if „freely given, specific, informed and explicit."[67] Consent is not given freely in the event the data subject has no „genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment."[68] In addition, consent according to GDPR(p2012), Article 7 para. 4 forms not a legal basis, if there is „significant imbalance between the position of the data subject and the controller". The prime example for such a significant imbalance is the employment relationship, as recognized by GDPR(p2012), Whereas (34). Therefore, consent as a basis for the Handling of employment related data will in the future likely not only be made „more difficult",[69] but practically impossible.

While it might not be possible to get valid consent from all data subjects, it might make sense seeking it to the extent practically and legally possible. The Handling of Personal Data covered by valid consent reduces the volume of Personal Data for which a different legitimization is required. As the volume of the information is relevant with respect to the balancing of the respective interests, a positive influence on the overall evaluation might be the consequence. It seems that, along these lines, some defendants solicit consent from those data subjects that receive litigation hold letters.

3. Two-step approach: General Requirements and Specific Export Requirements

The evaluation of the Handling of „German" Personal Data with respect to U.S. litigation requires a two-step approach. Initially, as each and every step in the Handling chain requires specific permission, this general requirement has to be met. In addition, in the event Personal Data is exported to a third country, additional specific requirements set forth in Section 4b and 4c BDSG have to be fulfilled. In essence, it is evaluated if the Handling would be legitimate if the litigation was purely intra-European on the first level, while on the second level it is evaluated if the Export of Personal Data is in line with German and European Data Privacy laws.

In its working document from 2009 on pre-trial discovery for cross border civil litigation the *Article 29-Working Party* („*Working Party*") has proposed solutions for each Handling step. The working document operates on the presumption that demands of the litigation process in a foreign jurisdiction have to be reconciled with the data privacy obligations of the Directive.[70] The working document states explicitly that „the Directive does not prevent transfers for litigation purposes" but that „there must be compliance with certain data protection requirements" and proposes respective guidelines.[71] As stated by it, the conflict has to be resolved „on a governmental basis, perhaps with the introduction of further global agreements along the lines of the Hague Convention."[72] While the *Working Party* does not have any legislative authority, of course, it can be expected, that the relevant EU and national authorities carefully examine and consider its recommendations in this highly volatile area of law.[73]

4. General Handling Requirement: Safeguard Controller's Legitimate Interest

Part one of the two-step approach requires the meeting of the general Handling requirements set forth in Section 28 BDSG.[74] Pursuing own commercial purposes will more likely than valid consent legitimize the Handling of Personal Data for transcontinental litigation. According to Section 28 para. 1 sentence 1 numeral 2 BDSG, Handling is lawful „[…] as a means to pursue own commercial purposes […] as far as necessary to safeguard legitimate interests of the controller and [if] there is no reason to assume that the data subject has an overriding legitimate interest […]."

It needs to be noted that Section 32 BDSG – that deals with data Handling for employment related purposes – is in general not applicable in the context of general business litigation. According to the legislative intent, Section 32 para. 1 BDSG permits the Handling if it is necessary for the decision to hire the data subject, or for carrying out the employment contract as well as for

59 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4a, marginal 3; *Pröpper/Römermann*, MMR 2008, 514, 515 f.
60 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4a, marginal 42 with further reference.
61 Section 4a para. 1 sentence 2 BDSG.
62 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4b, marginal 4.
63 The legislator's reasoning, specifically discussing employment situations, sets forth that in case where pressure may be exerted, the consent has to be given without compulsion ("ohne Zwang"), published in: *Simitis/Dammann/Geiger*, Dokumentation zum Bundesdatenschutzgesetz, p. 108.
64 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4b, marginal 9.
65 According to the *Hamburg Commissioner for Data Protection* employees may generally lack independence to effectively consent at all (22. Report of the Commissioner, p. 95; 18. Report of the Commissioner, p. 197).
66 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4b, marginal 23 with reference to principles set forth in *BGH* DB 2008, 2188, 2189 = MMR 2008, 731 m. Anm. *Grapeutin*.
67 GDPR(p2012), Article 4 para. 8.
68 GDPR(p2012), Whereas 33.
69 *Kunert*, 11 PVLR 06, 6.
70 *Working Party*, WP 158, p. 2.
71 *Working Party*, WP 158, p. 7.
72 *Working Party*, WP 158, p. 2.
73 *TSC*, International Overview 2009 – Germany, p. 103.
74 The particularities with respect to the Handling of Sensitive Personal Data are dealt with in Chapter III.8.

its termination and winding-up.[75] Therefore, Section 28 para. 1 sentence 1 numeral 2 BDSG remains applicable as far as the purpose of the Handling is not employment related but related to the controller's own (other) interests; in this case general business litigation.

a) Legitimate Interest

The application of Section 28 para. 1 sentence 1 numeral 2 BDSG requires the existence of a legitimate interest of the controller.[76] Any legal, economic and even ideational interest suffices in this regard.[77] Hence, the defense against a lawsuit directed against the data controller, even in a foreign country, is a legitimate interest in this sense.[78] The interests of justice would not be served by unnecessarily limiting the data controller's ability to promote or defend its legal rights.[79] This understanding is fostered by the fact that Section 28 para. 6 numeral 3 BDSG even makes the Handling of Sensitive Personal Data (Section 3 para. 9 BDSG) lawful to assert, exercise or defend legal claims unless there is an overriding interest of the data subject.

The Handling is necessary, if the legitimate interest cannot – or at least not in a reasonable other way – be met.[80] According to *Brisch/Laue*,[81] a strict necessity requirement is posted by the statute. Obviously, effectively defending ones rights in foreign litigation requires compliance with the lex fori.

b) Proportionality: Balancing the Interests

It is not sufficient, however, that a legitimate interest of the controller exists to allow for any and all Handling of Private Data. One dogmatic indication for further restrictions is that only Handling is permitted, that is „necessary to safeguard" the respective interest. In addition, the statute itself requires in Section 28 para. 1 sentence 1 numeral 2 BDSG that „[...] there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of processing or use [...]."

The GDPR(p2012), Article 6 para. 1 (f) sets forth in the same vein, that there can be no overriding interests or fundamental rights of the data subject, which require protection of Personal Data. In addition, the GDPR(p2012) contains an explicit right to object for the data subject, which can be overridden by „compelling legitimate grounds for processing" only (Article 19 para. 1).

There is little guidance as to what constitutes such an overriding interest in the context of transcontinental litigation. In general, the private sphere and the intimate sphere of the data subject have to be protected. Economic and professional detrimental effects as well as an influence on the reputation can be relevant factors, too.[82] While the data controller – in a summary evaluation[83] – should not have reason to believe that legitimate interests of the data subject override its legitimate interest in the event the properly informed data subject does not object to the Handling, the Handling in itself always has to be proportional. The Handling of Personal Data must, in other words, never be excessive.

In the end, the evaluation comes down to a balancing test between the controller's legitimate interests and those of the data subject („Balancing Test"). This is not only the current understanding of the law, but will be sustained under the GDPR(p2012) as exemplified in the Memorandum(2012), which states that Export „may, under limited circumstances, be justified on a legitimate interest of the controller [...] but only after having assessed [...] the circumstances of that transfer operation."[84]

In general, proportionality, relevancy for litigation, and potential consequences for the data subject have to be considered.[85] As stated by the *Working Group* it is clear that „both the U.S. and the EU legal systems place importance on the proportionality and the balance of the rights of the different interests."[86] Viewed in the light of the general principles of data privacy law set forth in Section 3a BDSG – data reduction and data economy – only the Private Data absolutely required to defend against the foreign law suit is covered.[87] Balancing the relevant interests asks for more than trying to minimize the effort of the data controller with respect to its legitimate interest; the aim is to allow the data controller to pursue such interests with the least Handling of Personal Data and the least intrusion into the data subject's rights.[88]

Naturally, trying to find a proportional solution asks for a fact-driven, case-by-case analysis with respect to each step. This analysis will be done in the subsequent chapters, specifically for each step of the Handling chain.

c) Involvement of Service Providers

In many instances, the data controller will not have the resources or know-how to conduct the Handling all by itself. In the event the data controller does the Handling, its own commercial purpose can legitimize the Handling in accordance with Section 28 para. 1 sentence 1 numeral 2 BDSG. Provided that the Handling by the data controller itself is legitimized by this section and provided that no Export occurs, the Handling by the service provider on behalf of the data controller is legitimized relating to substantive law by this section, as well. The service provider within the European Economic Area stands within the sphere of the data controller having the consequence that a „transfer" to it does not require a separate legal basis.[89]

According to Section 11 para. 2 BDSG the data controller shall choose the service provider carefully and with special attention to the suitability of the technical and organizational measures applied by it. The scope of the work to be done by the service provider shall be specified in writing. In addition, Section 11 para. 2 sentences 4 and 5 require the data controller to verify compliance especially with respect to data protection and respective proper documentation.

It should be noted that GDPR(p2012) sets forth extensive requirements for the data processor explicitly in its Article 26, which in essence reflect the currently valid law in Germany (Section 11 BDSG).

---

75 Recommendation of the *Committee on Internal Affairs of the Deutscher Bundestag*, BT-Drs. (document of the *German Bundestag*) 16/13657, p. 20 f.

76 The issue if a legitimate interest exits, if litigation is directed not against the controller but against a group company, is not discussed in detail in this publication. However, according to *Brisch/Laue*, the legitimate interest of a group company is not sufficient; *Brisch/Laue*, RDV 2010, 1, 4. The *Working Party* seems to allow for transfer of data by the EU subsidiary of the sued foreign parent company; *Working Party*, WP 114, p. 15; *Hanloser*, DuD 2008, 785, 786 seems to prefer the later view.

77 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. Supplement 2011, Section 28 BDSG, marginal 230; Däubler/*Wedde*, BDSG Kompaktkommentar, 3. Edition 2010, Section 28, marginal 48.

78 *Brisch/Laue*, RDV 2010, 1, 4; *Spies/Schröder*, MMR 2008, 275, 278.

79 *Working Party*, WP 158, p. 9.

80 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. Supplement 2011, Section 28 BDSG, marginal 235; Simitis/*Simitis*, BDSG, 7. Edition 2011, Section 28, marginal 108.

81 *Brisch/Laue*, RDV 2010, 1, 4.

82 *Gola/Schomerus*, BDSG, 10. Edition 2010, Section 28, marginal 35.

83 Simitis/*Simitis*, BDSG, 7. Edition 2011, Section 28 BDSG, marginal 129.

84 Memorandum(2012), p. 12.

85 *Brisch/Laue*, RDV 2010, 1, 6; *Working Party*, WP 158, p. 11.

86 *Working Party*, WP 158, p. 10.

87 Data Warehousing and Data Mining, e.g., therefore are not generally covered, Däubler/*Wedde*, BDSG Kompaktkommentar, 3. Edition 2010, Section 28, marginal 50).

88 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. Supplement 2011, Section 28 BDSG, marginal 239; Simitis/*Simitis*, BDSG, 7. Edition 2011, Section 28 BDSG, marginal 129.

89 Section 3 para. 8 sentence 3 BDSG.

5. Specific Requirement for the Export of Personal Data to the U.S.

Part two of the two-step approach requires the meeting of specific requirements to legitimize any Export of Personal Data. The rationale behind the European data privacy regime requires that the rights and interests of the data subjects are not jeopardized due to the fact of any Export. Therefore, the same level of protection has to be ensured, even if the Personal Data leaves the womb of Europe. Besides the general axioms of data privacy laws,[90] Section 4b BDSG and Section 4c BDSG apply, which set forth additional Export specific requirements.[91]

In general, Personal Data shall not be transferred to third countries (non-European Union Member States and non parties to the Agreement on the European Economic Area), if such third country fails to ensure an „adequate level of data protection."[92] Currently, the U.S. has to be considered as not providing the required adequate level of protection.[93]

However, the BDSG provides several alternatives to legitimize a data Export to the U.S. The mechanisms shall ensure that the data subject receives adequate protection in a specific instance despite the general lack of „adequate level of data protection".

a) Safe Harbor Scheme

With the *European Commission's* Decision 2000/520/EC a U.S.-specific way of allowing Exports to the U.S. was established between the *Commission* and the *U.S. Department of Commerce*. An adequate level of data privacy is considered to be ensured by organizations established in the U.S. that follow the Safe Harbor Privacy Principles implemented in accordance with the guidelines provided by the frequently asked questions issued by the *U.S. Department of Commerce* (Article 1 of the EC Decision).

While certain internationally active law firms are (self-)certified „Safe Harbors",[94] it seems unlikely that especially opposing party and U.S. courts can and will submit themselves to this regime.[95]

b) Transfer Contract

In the event the third country neither ensures an „adequate level of data protection" nor the Safe Harbor Privacy Principles can be implemented, the competent national supervisory authority may authorize a transfer of Personal Data to bodies, where the controller adduces adequate safeguards with respect to the protection of data privacy and exercise of the corresponding rights. Section 4c para. 2 BDSG sets forth the respective options.

One possibility to ensure adequate safeguards is the entering into a Transfer Contract. The *European Commission* issued several decisions relating to standard clauses for such a Transfer Contract.[96] In a press release dated 7 January 2005 the *European Commission* stated that „use of standard contractual clauses offers companies [...] a straightforward means of complying with their obligations [...] to ensure 'adequate privacy' for personal data transferred outside of the EU."[97] The member states' national authorities have to recognize that these transfers ensure adequate privacy.[98]

While Section 4c para. 2 sentence 1 BDSG states that a permit is required, a majority of commentators seem to believe that merely informing the national authority is sufficient and, as long as the standard clauses are used in an unmodified form, any additional requirement would constitute a dispensable formality.[99] Following this approach, even the requirement to inform the competent authority is dispensable and would likely violate the principle of proportionality.

From a practical perspective, it seems advisable however to inquire the position of the competent authority with respect to its view on information and permission requirements in this context. Allegedly some authorities outside of Germany have a different and strict position. Therefore, it is suggested to inform the national authority accordingly, state explicitly that it is understood that a permit is not required, and ask for notification if the authority is of a different opinion. It goes without saying that a specific deadline should be set and that no Export should be conducted before the specified time.

In the event of derogations from the standard clauses, a special permit needs to be obtained, of course.

Prior to transferring Personal Data, it has to be verified that the foreign recipient cannot be forced in the foreign country to violate the Transfer Contract. If such verification fails, the protection of the data subject requires that Transfer Contracts cannot legitimize the respective Export.[100]

In summary, with respect to transfers to the foreign outside counsel and service providers, the entering into Transfer Contracts may provide a viable starting point.[101] According to some commentators, those are even usually entered into between the data controller and its outside counsel.[102] It should be noted that the *Working Party* even suggests that ensuring data privacy by way of using the Safe Harbor Scheme, Transfer Contracts or „a convention" should be considered prior to making use of legislative exceptions, which will be discussed below.[103] Transfers that might be qualified as repeated, mass or structural are recommended to occur within a specific legal framework.[104]

However, with respect to opposing counsel and U.S. courts, it seems unlikely that those can and will enter into respective Transfer Contracts.[105]

c) Binding Corporate Rules

Corporate groups may establish binding corporate rules („BCR") to ensure the required protection of data privacy even if an Export occurs. BCR are one option explicitly set forth by the BDSG with which the controller can „adduce adequate safeguards" as required by Section 4c para. 2 sentence 1 BDSG.[106]

The BCR must be binding within the group as well as to the outside world. As a general rule, the BCR have to ensure a like level of data privacy as the Transfer Contracts, as they should be con-

90 As discussed in Chapter III.4 and Chapter III.8 with respect to Sensitive Personal Data.

91 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. Supplement 2011, Section 4c BDSG, marginal 19.

92 Section 4b para. 2 sentence 2 BDSG.

93 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4b, marginal 15; *Brisch/Laue*, RDV 2010, 1, 6; *Spies*, MMR 7/2007, p. V, VII; *TSC*, International Overview 2009 – Germany, p. 102. In addition, the European Commission's Decision 2000/520/EC would entirely be unnecessary if one would believe the U.S. provides the required protection.

94 The respective list is available under: https://safeharbor.export.gov/list.aspx.

95 *Brisch/Laue*, RDV 2010, 1, 6; *Hanloser*, DuD 2008, 785, 788.

96 See 2001/497/EC, 2002/16/EC (repealed by 2010/87/EU), 2004/915/EC and 2010/87/EU.

97 Press Release of the *European Commission*, IP/05/12.

98 See Commission Decision 2010/87/EU, Recital (5); Memo of the *European Commission*, Memo/10/30, p. 1.

99 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. Supplement 2011, Section 4c BDSG, marginal 23; Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4c, marginal 18c with further reference.

100 Such evaluation with respect to the U.S. lies outside the scope of this publication.

101 *Brisch/Laue*, RDV 2010, 1, 6.

102 *Spies/Schröder*, MMR 2008, 275, 279.

103 See Chapter III.5.d) and III.5.e).

104 *Working Party*, WP 114, p. 9.

105 *Brisch/Laue*, RDV 2010, 1, 6.

106 According to another view, BCR establish an adequate level of data protection within the meaning of Section 4b para. 2 sentence 3 BDSG. Respective Exports would not require authorization accordingly.

sidered as intra-group Transfer Contracts.[107] BCR are available only to affiliated enterprises.[108]

In the event, an Export covered by BCR is to occur, it has to be approved by the competent authority.[109] Section 4c para. 2 sentence 1 BDSG states that authorization is required and as no standard BCR are established yet, such permission is not a mere formality. While the BCR itself do not have to be approved, an informal procedure of reconciliation of BCR between the national supervisory authorities is established. The national authorities compare the level of data privacy established by the Directive to the level created by the BCR and therewith determine if adequate safeguards are adduced.

Certain internationally active companies might have such BCR in place.[110] However, they do not provide a means to legitimize the Export from a European controller, who is a party to U.S. litigation, to its outside counsel in the U.S.

d) Compliance With Legal Requirement

Another option set forth in the Directive (Article 26 para. 1 (d)) permits Export in the event, the data transfer is „necessary or legally required on important public interest grounds".

The BDSG[111] does not set forth the „legally required" exception explicitly.[112] To ensure compliance with the Directive, it is suggested that this option is considered to be one of the „important public interest grounds" provided for in Section 4c para. 1 numeral 4 BDSG.

Legal obligations arising out of a foreign statute or regulation do not qualify as „legal obligation" within the meaning of this Section, by virtue of which the Export could be permitted. The same is true for a foreign court order. Data privacy within the European Union cannot be consigned or even be dependent on legislative actions of non-member state governments. The relevant decision as to important public interest grounds has to be made by national legislation applicable to data controllers in the EU, not by foreign authorities.[113] The GDPR(p2012) makes this point even clearer and explicitly requires that the obligation has to be provided for in „Union law or law of the Member State,"[114] even if the foreign law „purport[s] to directly regulate data processing activities."[115]

Compliance with a request made under the Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters („Hague Evidence Convention") could theoretically provide a formal basis for the export of Personal Data.[116] The Hague Evidence Convention establishes methods of co-operation for the taking of evidence abroad. It applies only between signatory states. One signatory state may by means of Letters of Request ask the competent authority of another signatory state to obtain evidence. The *Working Party* stated that where it is possible, the Hague Evidence Convention should be considered first as a method of providing for Export of information for litigation purposes.[117]

While the Hague Evidence Convention allows for the request for pre-trial discovery of documents, many signatories such as Germany, France, Spain, and the Netherlands – inline with Article 23 of the Hague Evidence Convention – declared „that [they] will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries".[118] Hence, the German Competent Authorities will generally not process any requests under the Hague Evidence Convention for production of documents.[119] Therefore, the Hague Evidence Convention can currently not provide a basis for a legitimate Export of Personal Data protected by German data privacy laws to the U.S.[120] It needs to be noted that the protections offered by the Hague Evidence Convention are far from effective in the U.S. in any event.[121]

However, modifications to the Hague Evidence Convention or of the German implementation law could de lege ferenda ease the dilemma discussed in this publication. While it would entail a long and stony road, it might be worth the effort. This is especially true, as a modified Hague Evidence Convention could reach two goals: establish a basis for the Export of Private Data for transcontinental litigation purposes as well as guarantee its thorough actual acceptance and application in the U.S. Discussions and consultations for the Hague Evidence Convention II should be started on an international level.[122]

e) Necessity Related to Legal Claims

Another way to legitimize the Export of Personal Data to a third country is set forth in Section 4c para. 1 numeral 4 BDSG. This statutory exception applies, if the „transfer is necessary for the establishment, exercise or defense of legal claims."

This section reflects the understanding that the data controller's ability to promote or defend a legal right should not be unnecessarily limited.[123] While not tested in German courts,[124] this exception allows for the transfer of Personal Data not only to the court but also to all those involved in the litigation process as it would be meaningless otherwise.[125]

---

107 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4c, marginal 22; *Hanloser*, DuD 2008, 785, 788.

108 *Hanloser*, DuD 2008, 785, 788; according to *Däubler* Section 15 Aktiengesetz (German Stock Corporation Act) is decisive in that regard (Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4c, marginal 24).

109 *Kunert*, 11 PVLR 06, 9 assumes that currently specific authorization is required, as the abandonment of this requirement is a „great boon".

110 Däubler/*Däubler*, BDSG Kompaktkommentar, 3. Edition 2010, Section 4c, marginal 24; the link set forth could not be verified, however.

111 It needs to be noted that the translation provided by the *Federal Commissioner for Data Protection and Freedom of Information* does not reflect that distinction between the Directive and the BDSG, available under: http://www.bfdi.bund.de/cae/servlet/contentblob/844438/publicationFile/51362/aktualisiertesBDSG.pdf.

112 The German versions read as follows:
Article 26 para. 1 (d) Directive:
„die Übermittlung [...] für die Wahrung eines wichtigen öffentlichen Interesses [...] erforderlich oder gesetzlich vorgeschrieben ist."
§ 4c para. 1 sentence 4 BDSG:
„die Übermittlung [...] für die Wahrung eines wichtigen öffentlichen Interesses [...] erforderlich ist."

113 *Working Party*, WP 114, p. 15; *Working Party*, WP 158, p. 9.

114 GDPR(p2012), Article 6 para. 1 (c) (3).

115 GDPR(p2012), Whereas 78, 90.

116 *Brisch/Laue*, RDV 2010, 1, 6; *Working Party*, WP 158, p. 13.

117 *Working Party*, WP 158, p. 14.

118 See Section 14 of the German implementation act (Ausführungsgesetz zu den Haager Reformübereinkommen von 1965 und 1970).

119 *Hanloser*, DuD 2008, 785, 786. The German section in *TSC*, International Overview of Discovery, Data Privacy & Disclosure Requirements states on p. 95 that „in some cases, the German Central Authorities may pass Letters of Request on to the German local courts if the U.S. court requests specific documents from the party or non-party in Germany, the documents are necessary for rendering a decision and the U.S. court proceeding is already pending." Any such assistance would violate German law however, as the executive order law, which would be required for such assistance in accordance with Section 14 para. 2 of the German implementation act, does not exist.

120 *Brisch/Laue*, RDV 2010, 1, 6.

121 This is true as (a) U.S. courts consider compliance with the Hague Evidence Convention not mandatory; it is a means of obtaining evidence abroad but not the only one. Given this understanding, the Hague Evidence Convention is an option, the plaintiff can choose to make use of. Needless to say that this renders the Hague Evidence Convention basically pointless, *Working Party*, WP 158, p. 7; (b) defendants frequently „voluntarily" co-operate with plaintiffs to avoid negative implications in the U.S. proceedings; and (c) defendants frequently themselves request production of documents; see *Working Party*, WP 158, p. 9.

122 *Knöfel* opines that discovery requests should be dealt with regularly within the framework of the Hague Evidence Convention, RIW 2010, 403, 406.

123 See already Chapter III.4.

124 *TSC*, International Overview 2009 – Germany, p. 103.

125 *Spies/Schröder*, MMR 2008, 275, 279; *TSC*, International Overview 2009 – Germany, p. 103.

Reading the statute, one might wonder, if any additional requirement is postulated by this clause in the context of foreign litigation at all. The (broader) general requirement for any Handling in this context as set forth in Section 28 BDSG allows for Handling if „[...] necessary to safeguard legitimate interests of the controller [...]." Certainly, establishment, exercise or defense of legal claims constitutes such a legitimate interest.

Light might be shed on the interplay between those two clauses by the following: Generally, from a data privacy perspective, the Export of Private Data to third countries with a less stringent data privacy system than required in all the member states is disfavored. Viewed in this context, Section 4c para. 1 BDSG provides exceptions from the general principle that the Export to third countries is only to occur if an adequate level of protection under the given specific circumstances is ensured by other means. The exceptions acknowledge that the expansion of international trade requires flexibility on certain occasions.[126] However, the exceptions have to be applied restrictively and in a way to compensate for the lack of an adequate level of data privacy.[127]

While some scholars state that the interests of the data subject regularly speak against the Export,[128] such a fundamental approach does not seem to be in line with the recognized need for flexibility within global trade. In addition, such an approach might in the end be detrimental to the aim to protect Private Data. This might especially be true if the respective U.S. court assumes that the national data privacy regime represents a blocking statute and is virtually ignored. Finding mutually acceptable solutions requires, in line with the TSC International Principle I, paying due respect to the respective other legal system.[129] Therefore, if applied restrictively Section 4c para 1 sentence 4 BDSG is correctly seen by most sources as authorizing the transfer of Personal Data to local counsel, litigation service providers, opposing counsel and the court.[130]

To ensure the restrictive application, in other words the proportionality of specifically the Export, an additional Export oriented Balancing Test („Export Balancing Test") has to be performed, similar to the one to satisfy the general Handling requirements according to Section 28 BDSG.[131] However, one has to keep in mind, that the transfer of Personal Data to a country that does not ensure adequate data privacy is seen as jeopardizing the data subject's privacy rights to a higher degree. Just to name one reason: Absent a protective order, the court file is – in sharp contrast to the ideas of EU data privacy – generally accessible to the public in the U.S.[132] Therefore, the bar to allow data Exports has to be raised, once such a country comes into the equation; the scale initially tips on the side of non-transfer.

6. Export Related Balancing Test

The last chapter concluded that in the event the „necessity with respect to legal claims" exception is made use of, an Export Balancing Test has to be performed. This requirement is not limited to the „legal claim exception" however, but applicable in the event a Safe Harbor or a Transfer Contract is used, as well.

While the data controller can, using Safe Harbors or Transfer Contracts, ensure that an „adequate level of data protection" exists in general, the data subject can have a legitimate interest in ruling out the possibility of the Export nevertheless. A first indication of this result is the wording of Section 4b para. 2 sentence 2 BDSG: such legitimate interest may exist „especially if the bodies [...] fail to ensure an adequate level of protection". The wording indicates that other reasons may exist. In addition, the factor that such Exports are generally disfavored was mentioned previously.[133] Moreover, the Directive (Article 25 numeral 1) assumes that besides the general and specific requirements with respect to a specific Export, the overall level of data privacy of the third country is to be evaluated. Without the Export Balancing Test, this would not be guaranteed.

Hence, the unlimited transfer of all Personal Data to the U.S., meeting the general Handling requirements and formal specific Export requirements, is not in line with German and EU data privacy laws. The Export Balancing Test has to be satisfied prior to any Export to legitimize the same. The particularities of the Export Balancing Test will be discussed at the relevant step of the Handling chain.

7. GDPR(p2012): Export Balancing Test Still Required

The GDPR(p2012) still follows the two-step approach, as set forth by its Article 40. General as well as specific requirements will still have to be complied with. On the general level, the Handling is lawful if the „processing is necessary for the purpose of the legitimate interest pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data".[134] Clearly, a Balancing Test is to be passed before the Handling can be classified as legitimate with respect to the general requirement.

With respect to the requirement of an Export Balancing Test the wording is less clear. Three options for a lawful Export are set forth by the GDPR(p2012): an adequacy decision with respect to the third country,[135] which is not applicable and not to be expected with respect to the U.S.;[136] appropriate safeguards by way of legally binding instrument or prior authorization by the competent authority;[137] or a derogation, in this context in the form of an Export „necessary for the establishment, exercise or defense of a legal claim".[138] There is no indication whatsoever, that the existing general and specific Export requirements should be softened with the GDPR(p2012) taking effect.

Quite the contrary seems to be true and can be exemplified by changes made on short notice before the publication of the GDPR(p2012). As set forth by the respective memorandum (p. 12), Article 42 of the inter-office version 56 („GDPR(p2011_56)") clarified that a controller is prohibited to disclose Personal Data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority. While the respective Article is not included in the GDPR(p2012), the *Commission* has stated publicly that it may adopt restrictions on transfers compelled by foreign courts or governmental authorities.[139] The general *Commission's* tendency is clear: the Export

126 Directive, Recital (58).
127 Taeger/*Gabel*, BDSG, Section 4c, marginal 5; see with respect to the Directive *Working Party*, WP 114, p. 7.
128 *Bergmann/Möhrle/Herb*, Datenschutzrecht, 43. Supplement 2011, Section 28 BDSG, marginal 245.
129 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 7.
130 *Brisch/Laue*, RDV 2010, 1, 7; *Spies/Schröder*, MMR 2008, 275, 279; *Hanloser*, DuD 2008, 785, 788 and others; for the contrary view see footnote 128.
131 See Chapter III.4.b).
132 *Rath/Klug*, K&R 2008, 596, 598.
133 See, inter alia, Chapter III.5.
134 GDPR(p2012), Article 6 para. 1 (f).
135 GDPR(p2012), Article 41 para. 1.
136 In accordance with GDPR(p2012), Article 41 para. 5 and para. 6 the *Commission* may take a „non-adequacy" decision, in which case transfers shall be prohibited without prejudice to Articles 42 to 44.
137 GDPR(p2012), Article 42 para. 1.
138 GDPR(p2012), Article 44 para. 1 (e).
139 *Kunert*, 11 PVLR 06, 10.

to the U.S. for litigation purposes is certainly not favored and the underlying requirements will not be softened.

It is therefore unlikely that the *Commission* has any desire to abandon the Export Balancing Test. This view is underpinned by the Memorandum(2012) that states explicitly that „international data transfer may, under limited circumstances, be justified on a legitimate interest of the controller [...] but only after having assessed and documented the circumstances of that transfer operation."[140] This statement represents another indication that the Export Balancing Test will still be required in the future. To foster this aim, it is suggested to include the respective wording into the final regulation or the respective memorandum, at least.

8. Handling of Sensitive Personal Data for Transcontinental Litigation

Sensitive Personal Data enjoy special safeguards due to the data subject's heightened interest in their protection.[141] In the event such data is to be handled in connection with transcontinental litigation, Section 28 para. 6 to para. 9 BDSG supersede Section 28 para. 1 BDSG.

Section 28 para. 6 numeral 3 BDSG legitimizes the Handling on the first, general level, if it is „necessary to assert, exercise or defend legal claims and there is no reason to assume that the data subject has an overriding legitimate interest in ruling out the possibility of" the Handling. Hence, „necessity with respect to legal claims" can generally legitimize even the Handling of Sensitive Personal Data, provided it is proportional. In this case, the Balancing Test has to accommodate for the fact of the special sensitivity of the data[142] as well as the intention of the EU legislator to especially safeguard data falling into this category.

On the second level, the specific requirements, e.g., as set forth in Section 4c para. 1 numeral 4 BDSG, can legitimize the Export of the Sensitive Personal Data.[143] The required Export Balancing Test has to take the special need for protection of the data in consideration, as well.

In essence, the special need for protection of the Sensitive Personal Data has to be taken into account when evaluating each step of the Handling chain and when putting special safeguards into place.

9. Involvement of the Data Protection Officer

While there is no affirmative obligation under the BDSG,[144] it is „standard procedure" in many discovery cases to actively involve the data protection officer („DPO") of the controller. If the DPO learns about a specific matter and wants to get involved, he is entitled to such involvement. Such involvement has the benefit that the DPO can consult with the national authority to ensure that no violations with respect to national data privacy laws occur.[145] In addition, it might seem odd to an U.S. court to fail to enlist the assistance of the DPO, while its assistance and „blessing" might shine a positive light on the controller's conduct if a discovery dispute arises. It shows the controller's good faith if the U.S. court or a national authority ever challenges its actions.

Therefore, while the involvement is not mandatory, it seems good practice to include the DPO as soon as reasonably possible. Under the regime of the GDPR(p2012) such involvement will be mandatory.[146]

10. Transparency

According to the *Working Party*, the Directive requires advanced general notice of the possibility of Personal Data being handled for litigation purposes.[147] In the event Personal Data is actually handled for litigation purposes, notice should be given of the identity of any recipients, the purpose of the Handling, the categories of Personal Data concerned and the existence of the data subject's rights.[148]

Such a general requirement seems too broad and not generally manageable. Just as it is very difficult to obtain consent from all data subjects in major litigation, it would be very hard to properly inform all data subjects. Therefore, the specifics of this requirement need to be determined with respect to each step of the Handling chain. One of the decisive factors will be if the Personal Data was already pseudonymized or anonymized.

11. Rights of Access, Rectification and Erasure

Once notified, the data subjects have the right to access their Personal Data, as well as to rectification and erasure, if certain requirements are met. While the *Working Party* correctly notes that those rights „could give rise to a conflict with the requirements of the litigation process to retain data, as at a particular date in time and any changes (whilst only for correction purposes) would have the effect of altering the evidence in litigation",[149] it seems that in collaboration with the opposing party and, if necessary, the U.S. court overseeing the litigation, solutions should be feasible.

From a practical perspective, once any request for rectification or erasure is made, the respective Personal Data should, in line with the International Principle 4,[150] be separated from the other data, whereupon a solution should be negotiated with the opposing party or a decision requested from the U.S. court.

12. Data Protection

The data controller has to take reasonable technical and organizational precautions to preserve the security of the Personal Data and hence provide an acceptable level of data protection. The level of security has to be appropriate to the risk represented in the specific instance.[151] It has to impose those requirements on law firms dealing with the Personal Data as well as litigation support service providers and others. It seems that the data controller remains responsible for the Handling operations of external service providers and has to periodically verify compliance with the data protection rules.[152]

Moreover, preserving the security of the Personal Data could also include „a requirement for sufficient security measures to be placed upon the court service in the relevant jurisdiction as much of the Personal Data relevant to the case would be held by the courts for the purpose of determining the outcome of the case."[153] Such a requirement places an interesting burden on the data controller. It seems that the data controller cannot be forced to do more than ask the respective U.S. court for appropriate protection. In any event, it should document the respective steps and efforts.

---

140 Memorandum(2012), p. 14.
141 See Chapter II.5.
142 Däubler/*Wedde*, BDSG Kompaktkommentar, 3. Edition 2010, Section 28, marginal 175.
143 See Chapter III.5.e).
144 As far as *Spies*, MMR 7/2007, p. V, VII, postulates a duty of the controller to involve the DPO, this view is not shared.
145 *TSC*, International Overview 2009 – Germany, p. 101; in the same vein *Working Party*, WP 158, p. 11.
146 GDPR(p2012), Article 36.
147 *Working Party*, WP 158, p. 11.
148 See in particular Chapter III.11.
149 *Working Party*, WP 158, p. 12.
150 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 17.
151 GDPR(p2012), Article 30 sets this forth explicitly.
152 *Working Party*, WP 158, p. 13.
153 *Working Party*, WP 158, p. 12.

13. Documentation

While the GDPR(p2012) sets forth significant and detailed documentation requirements, data controllers are well advised to establish documentation policies under the regime of the BDSG already. Having general policies in place – and documenting that those were actually followed – will show good faith on the part of the data controller and help defend its actions in front of national authorities or U.S. courts.

IV. Application I: Preservation

The developed principles and basic rules with respect to the Handling of Personal Data for transcontinental litigation purposes can now be brought to life. The focus of the following chapters will be upon the practical application with respect to each step of the Handling chain.

While Preservation constitutes Handling of Personal Data already, broad Preservation, including the creation of a backup copy, is allowed for. The extent of the legitimate Preservation as well as its commencement is oriented on the requirements of the lex fori. However, culling of the Personal Data is required as soon as an agreement with opposing party or a court order with respect to the scope of discovery is reached. Anonymization and pseudonymization is regularly not yet mandatory.

1. Preservation Constitutes Handling of Personal Data

Once U.S. litigation is reasonably anticipated or commences,[154] the U.S. – state and federal – rules of civil procedure require that information potentially containing Personal Data be identified, in most cases separated, and securely stored. Once this is done a volume of „Preserved Data" exists.

Under the regime of the Directive and consequently the BDSG – but contrary to the U.S. perspective –, the mere Preservation of Personal Data for litigation purposes is to be considered Handling. As a consequence, Preservation requires a specific permission,[155] as – obviously – in most instances, the Personal Data was not collected for the purpose of future litigation. According to the general principles of data reduction and data economy,[156] Personal Data has to be deleted, once it is no longer required for the initial non-litigation purpose. Deletion may be omitted, if a new permission covers further Handling; in this case the continued Preservation.

2. General Handling Requirement for Preservation: Legitimate Interest

Preservation constitutes Handling of Personal Data and therefore requires either consent or a specific permission. Consent at this stage is impracticable as the data was not collected for the litigation purpose – hence, initial consent will not exist – and as the data is not yet analyzed in-depth, the data subjects are not even determined – hence, consent is not practicably achievable from the unidentified data subjects. In addition, valid consent will most likely not be achievable from employees in any event.

As set forth above, the defense against a lawsuit, irrespective if pending in Germany or any other country, constitutes a legitimate interest of the data controller. The crucial issue lies in the question if proportionality, in the sense of the required Balancing Test with respect to each step, exists.[157] Balancing the rights of potentially affected data subjects and the legitimate interest of the data controller needs to aim for a solution that allows the data controller to pursue its defense while minimizing the intrusion into the data subjects' interests.

a) Culling of Personal Data

Attributing the proper weight to the data subjects' interests for the Balancing Test requires definition of the scope of data involved.

At the stage where Personal Data that was legitimately collected is preserved for litigation purposes, it seems acceptable to preserve a rather broad scope of allegedly relevant data.[158] In line with the U.S. discovery approach, this includes information, which by itself is not relevant but which is likely to lead to the discovery of relevant evidence. While the Preservation of Personal Data that already exists within the controller's sphere certainly is an intrusion into the data subject's rights, as the Personal Data exists for an extended period, such intrusion can be classified as rather mild. This is true despite the fact that any Handling increases the risk of accidental or criminal release of Personal Data. It seems that the *Bundesverfassungsgericht* (*BVerfG – Federal Constitution Court*) accepts the need for a staggered approach in principle. In a decision relating to an authority's right to seizure of e-mails, it allowed for a broader scope of e-mails covered initially as immediate separation of messages was impracticable. However, for later permanent and therefore more intrusive infringements it required the culling of e-mails as fast as possible and reasonable.[159]

A more stringent approach could harm the data controller's position severely. It might force a European party to U.S. litigation at the Preservation phase already to violate U.S. procedural rules, potentially even court orders and subject itself to severe sanctions in the U.S. This seems a too harsh consequence given the rather mild intrusion into the data subject's rights. Hence, while only Personal Data covered by respective obligations under the lex fori may be preserved, it seems acceptable at this stage not to force the data controller already to cull the Personal Data down to actually relevant information in the European understanding of the term.

However, the controller has to make sure that only Preservation occurs initially and that the Personal Data cannot be used for any other purpose. In addition, logical or even physical separation of the relevant data from the general business data of the controller should be considered to reduce the risk of any misuse even further.

In line with the general principles, the controller has a duty as soon as practicably possible and at any stage to take appropriate steps to limit the scope of the Preserved Data.[160] As soon as a common understanding with the opposing party or a respective order of the foreign court is reached – any Personal Data exceeding such scope has to be deleted.

The respective culling down process constitutes Handling as well. As it is directed towards reducing the volume of the Preserved Data it has to be evaluated in a favorable light given the overall principles of data reduction and data economy. The respective process rather fosters the aims of data privacy than jeopardizes it and is generally permitted.

b) No Anonymization and Pseudonymization Required (yet)

At the Preservation stage, it seems acceptable in the light of Section 3a BDSG to not anonymize or pseudonymize Personal Data

154 See Chapter IV.2.c).
155 *Working Party*, WP 158, p. 8.
156 See Chapter II.9.
157 See Parts III.4.a) and III.4.b).
158 It seems that *Brisch/Laue*, RDV 2010, 1, 4 come to this conclusion, as well.
159 *BVerfG* MMR 2009, 673, 678 m. Anm. *Krüger*.
160 The *Working Party* seems to follow this line, WP 158, p. 10.

already. While anonymization, which by definition is irrevocable, could subject the data controller to the same peril as culling down the Personal Data at that stage too far, (reversible) pseudonymization seems to be disproportionate to the desired purpose of data privacy at the stage where the Personal Data is still secured within the controller. While one could certainly argue to the contrary with respect to a specific fact pattern, this position is taken as it seems unreasonable and impracticable to anonymize or pseudonymize at that stage in general.

c) Commencement of Legitimate Interest

The obligation to preserve information in the U.S. commences no later than when litigation is imminent, in other words the filing of a legal action can be reasonably anticipated.[161] To enable the data controller to effectively defend itself in the U.S., it has to be allowed for under European data privacy law that Preservation begins at the same point in time.

The mere and unsubstantiated general possibility[162] that the data controller may be subject to some litigation someday however is not sufficient.[163] This understanding does not necessarily conflict with U.S. procedural rules, as a litigant does not have to fear sanctions by a U.S. court according to FRCP 37(e) if it destroyed electronically stored information („ESI") „as a result of the routine, good-faith operation of an electronic information system". Of course, once any preservation obligation commences under U.S. procedural law, all routine deletion processes have to be stopped.

3. Preserved Data: Additional Backup Copy

According to the U.S. rules of civil procedure, once a duty to preserve data commences, no relevant data may be deleted. On the other hand, under a European regime of data privacy, more and more culling down of the Preserved Data will be required. Hence, the data controller might be caught in the battle of the respective regimes. In the end, a U.S. court may second-guess the data controller's decision and order production of additional documents, which may no longer be existent, subjecting the data controller to severe sanctions.

Therefore, data controllers might be tempted to store a complete copy of the Preserved Data. Provided that access to such a copy is given only in the event of a corresponding U.S. court order, the existence of such a backup copy can be legitimized as proportionally fostering the data controller's legitimate interest. Though, no opinions of the supervisory authorities are available with respect to this issue.

It can be argued that this approach is still in line with the GDPR(p2012), despite its explicitly set forth limits in Whereas (30) and Article 5 (c). However, utmost care has to be taken with respect to data protection and the control that access will not be granted for any other purpose.

4. Specific Export Requirements

Preservation, as defined above, does not comprise Export of Personal Data to the U.S. Therefore, no additional specific Export requirements have to be met.

5. Data Protection Officer

As set forth above, and just as a reminder, the DPO should be involved at this stage already.[164]

6. Initiate Documentation

Once the first steps with respect to a new Handling chain are anticipated or taken, the documentation for this specific Handling chain should be initiated. Ideally, it is derived from and in-line with the enterprises' general data privacy policies. Good corporate practice for enterprises involved in transcontinental business operations and therefore potentially subject to transcontinental litigation strongly encourages setting up such policies. Those general policies should only provide a framework as violating one's own general policies is even worse than not having one.

V. Application II: Internal Review

No litigation can be carried into execution meaningfully, unless the Preserved Data is analyzed in detail. At a certain point in time, the Preserved Data has to be handled further to foster the legitimate interest. It is assumed that the Internal Review can be conducted without an Export of Personal Data.

The Internal Review may have the form of the above-stated culling after the scope of discovery is limited or sorting and analyzing the information to explore the facts and the background of the case. This is necessary to, e.g., evaluate the case and define defense strategies.

Such Handling can – and usually will – lead to a reduction as well as an enlargement of the involved Personal Data. Only after certain information is reviewed and analyzed will further custodians of information be identified and consequently more information gathered. While the data controller has to balance the relevant interests during each step along the way on a case-by-case basis, necessary internal Handling should in general not pose any additional issues. No special rules for the Preservation of this additional information exist beyond the results developed above.[165]

Given the still rather limited risk posed to the interests of the data subjects, it would be disproportional to require the data controller to take additional time and money consuming steps at this stage. It is the clear intent of the BDSG and the respective European legislative background to allow the controller to defend its rights in litigation and therefore to put itself in a position to successfully do so. Any Handling should be documented accordingly.

VI. Application III: External Review

Handling of Personal Data with respect to litigation not pending in the jurisdiction of the controller but in another country outside the EU, more precisely the U.S., spurred this publication. Certainly, some external transfers are ultimately necessary to engage successfully in U.S. litigation. For the purpose of this chapter it is assumed that the External Review, be it legal or on the IT side, entails the Export of Personal Data to the U.S.

From the perspective of the pursuance of legitimate interests within the meaning of Section 28 BDSG it makes no difference if the Personal Data is transferred to outside counsel in the jurisdiction of the controller or to one in another, potentially one with a less stringent data privacy regime, third country. However, the Export of the Personal Data to external counsel in the U.S. makes the equation a lot more challenging, as specific Export requirements have to be met.

External Review of the Personal Data by outside counsel, non-legal service providers, and experts is on the general level legiti-

161 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 2.
162 *Brisch/Laue*, RDV 2010, 1, 3; *Spies/Schröder*, MMR 2008, 275, 278; *Working Party*, WP 114, p. 15; *Working Party*, WP 158, p. 8.
163 The issue to what extent Handling is legitimate in the ordinary course of business, in this case protection against claims and lawsuits in general, is outside the scope of this publication.
164 See Chapter III.9.
165 See Chapter IV.

mate to the extent necessary to safeguard the data controller's own interest with respect to discovery and defense against the legal claim. With respect to any, including U.S., litigation any reasonable Handling within the E.U. will hardly ever be disproportional; data controllers in general lack the ability to perform the necessary – legal or technical – Handling themselves.[166] As soon as an Export is required, the Export Balancing Test will, in general, only be met in the event, all reasonably doable culling is done prior to the Export, the Personal Data is anonymized or pseudonymized in the E.U., and the data subjects are informed properly to the extent reasonable.[167]

1. General Handling Requirement for External Review: Legitimate Interest

The external review of the Personal Data is allowed for by Section 28 para. 2 numeral 1 in connection with Section 28 para. 1 sentence 1 numeral 2 BDSG in the event that it is necessary to safeguard the data controller's own interests, in other words if it is necessary to defend against a legal claim. It goes without saying, that the in-depth review and analysis of the Personal Data is required to enable the trial counsel in the U.S. to defend the data controller properly. The External Review is not only legitimate if necessary with respect to discovery but also with respect to the case itself. German as well as U.S. counsel for the data controller can, by and large, review the Preserved Data, unless it is obvious that the Preserved Data contains excessive and irrelevant Personal Data or the data controller would clearly be in a position to cull down the information further, to anonymize or pseudonymize the data without any fear of negative consequences. With respect to U.S. litigation this will hardly ever be the case.

The inclusion of a litigation service provider is also legitimate.[168] Hardly ever will a data controller be able to perform the necessary preparatory steps on the IT side without any external assistance.

Hence, just as the Internal Review, the External Review is legitimized as it safeguards the controller's legitimate interest.[169]

2. Export Balancing Test en Detail

In addition, the Export of Personal Data to the U.S. requires additional safeguards to be met, which are set forth in Section 4b BDSG and Section 4c BDSG. The level of scrutiny is relatively high, as the U.S. is currently considered as a country not ensuring an adequate level of data privacy. Consequently, such Export is generally disfavored;[170] the presumption against Export needs strong safeguards to be overcome. The following options exist in general: the Safe Harbor scheme, Transfer Contracts, and transfers relating to legal claims. As set forth above, all three options can provide a basis for the Export only if an Export Balancing Test is passed.[171] The Export is disfavored in all three scenarios and the exceptions have to be applied restrictively as it involves a transfer to a country not providing an adequate level of privacy. Therefore, the scale initially tips on the side of non-export. However, if the following preconditions are met, the transfer may be considered legitimate.

a) Pre-Transfer Culling of Personal Data

Once the Export of Personal Data is necessary, the scope of the Personal Data that absolutely requires such Export has to be evaluated and reduced. In other words, only after each and every step doable in Europe is done, may the remainder be exported. The data subject that has in most instances done nothing to avail itself to the U.S. courts has a legitimate interest to keep its data out of a third country to the extent possible. The culling process of the Personal Data to an absolute minimum has in general to be conducted within the jurisdiction of a country ensuring adequate data privacy.[172] This local process is generally indispensable.[173] This view is in line with an opinion from August 2009 of the *French privacy and data protection authority (CNIL)* (the „French Opinion"). According to the French Opinion, the data must be objectively assessed in the country where the data resides.[174] The *Bavarian DPA* has opined in this sense, as well.[175]

Only in very rare, and certainly hard to justify instances, may the culling be legitimately done in the third country, in this case, the U.S.; in essence, this may be the case if the request for local culling is unreasonable.[176] Provided that the data controller decides to perform the culling abroad, extensive documentation of the reasons is suggested as well as co-operation with the national supervisory authority. A contrary view, that could argue that only the foreign counsel can make the determination properly, would be too broad and would not do justice to the legitimate interests of each data subject and the system of data privacy in the European Union.

b) Pre-Transfer Anonymization and Pseudonymization

Given that the national and European legislators disfavor the Export of Personal Data to the U.S., one has to concede that the Export increases the risk of harm done to the interests of the data subjects exponentially. Therefore, a much higher emphasis has to be placed on all reasonably feasible mechanisms to protect such interests. One of the most effective safeguards is the anonymization or at least pseudonymization of the Personal Data. As a general rule, Personal Data may only be transferred, once they are anonymized or pseudonymized to the extent allowed for by the purpose of litigation and as long as the effort is not disproportionate to the desired purpose of the data subject's privacy. "In most cases it will be sufficient to transfer the Personal Data in a pseudonymised form with individual identifiers other than the data subject's name."[177] At the very least, the controller has to verify prior to the later transfer if such a possibility exists.[178]

If the particularities of the legal claim in question require the Export of Personal Data not even pseudonymized, detailed documentation is in order.

c) Transparency and Rights of Access, Rectification and Objection

It is questionable, if the Export of Personal Data to the U.S. requires additional transparency steps. According to the French

166 See Chapter VI.1.
167 See Chapter VI.2.
168 See Chapter III.4.c).
169 *Brisch/Laue*, RDV 2010, 1, 5; *Hanloser*, DuD 2008, 785, 787; *Spies/Schröder*, MMR 2008, 275, 278.
170 See Chapter III.5.
171 See Chapter III.6.
172 *Working Party*, WP 158, p. 11; *TSC*, for Analysis of Cross-Border Discovery Conflicts, p. 12.
173 *Brisch/Laue*, RDV 2010, 1, 7; it seems that this view is shared by *Spies*, MMR 7/2007, p. V, VII.
174 Délibération nº2009-474 du 23 juillet 2009 portant recommendation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dites de „Discovery."
175 *Bavarian DPA*, report 2009/2010, p. 71, available under: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht_2010.pdf.
176 *Brisch/Laue*, RDV 2010, 1, 5; it seems that *Hanloser* comes to the same conclusion, DUD 2008, 758, 787. Both, *Brisch/Laue* and *Hanloser* discuss this issue under the heading of necessity with respect to Section 4c para. 1 sentence 1 numeral 4 BDSG.
177 *Working Party*, WP 158, p. 11; it seems that the German supervisory authorities share this view; *Berlin DPA*, annual report 2006, p. 170, available under: http://www.datenschutz-berlin.de/attachments/140/Jahresbericht_2006.pdf?1175508324; and annual report 2007, p. 191, available under: http://www.datenschutz-berlin.de/attachments/438/Jahresbericht_2007.pdf?1207310269; *Bavarian DPA*, report 2009/2010, p. 71, available under: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht_2010.pdf.
178 *Brisch/Laue*, RDV 2010, 1, 6; *Spies/Schröder*, MMR 2008, 275, 280.

Opinion, data subjects have to be informed prior to the Export with respect to the particularities of the Personal Data, the entity responsible for the Handling, the facts of the legal action, the link requiring disclosure of the data pertaining to the Data Subject; whether the disclosure is mandatory or optional; the consequences for the Data Subject of refusing disclosure of the data; and how the data subject can exercise the right to access, modify, and oppose disclosure of the information. According to the French opinion, the Data Subject can be informed after the transfer only, if (a) informing the Data Subject jeopardizes the ability of the data collector to gather evidence, and (b) preliminary injunctive relief is necessary to prevent destruction of evidence. Both exceptions are generally not available in transcontinental litigation.

While the approach favoring transparency is shared in general, and data subjects should be informed, a proportionality test has to be implemented. Only those steps that can be reasonably required from the data controller are mandatory.

VII. Application IV: Production

Once Production of the information occurs, any remaining Personal Data is irrevocably released into the public domain, unless specific safeguards are put into place. Therefore, this final step in the Handling chain requires utmost scrutiny and the broadest protection for the data subject possible.

Therefore, pre-production culling, anonymization, or pseudonymization has to be extended even further, especially, if – in rare cases – this was not done prior to the External Review.[179] In addition, the data controller in principle has to obtain binding court orders with respect to discovery and suitable protective orders.[180]

1. General Handling Requirement for Production: Legitimate Interest

Finally, Production of Personal Data to opposing counsel, opposing experts and the U.S. court will inevitably be requested at some point of the U.S. litigation. As Section 28 para. 6 numeral 3 BDSG even allows for the Handling of Sensitive Personal Data within the meaning of Section 3 para. 9 BDSG to assert, exercise or defend legal claims, there is no doubt that the legitimate interest generally includes compliance with U.S. rules of civil procedure. Therefore, the data controller generally has a legitimate interest to produce Personal Data to the extent necessary.[181] This approach is followed by the GDPR(p2012), as well.[182] However, it is equally clear that culling of Personal Data to the absolute necessary minimum is required prior to production.

a) Pre-Production Culling of Personal Data

Any further culling that does not expose the data controller to any additional risk with respect to the U.S. litigation has to be done prior to production.

b) Pre-Production Anonymization and Pseudonymization

In the event, Personal Data was exported for External Review without prior anonymization or pseudonymization performed, utmost scrutiny has to be used to determine if such steps can be done prior to production.

c) Pre-Production Binding Court Order and Protective Order

Furthermore, the respective U.S. court has to be approached prior to the Production of Personal Data. In this regard, *TSC* International Overview of Discovery, Data Privacy & Disclosure Requirements states that „scholars and the Federal Data Protection Commissioner, however, require a binding court order to produce such information and the scope must be limited to the extent absolutely necessary for the compliance with such order".[183]

In addition, parties may have to seek protective orders in order to limit the disclosure of the submitted information only to the necessary recipients.[184] It is therefore necessary to approach the U.S. court in each instance, explain the data privacy obligations upon the controller and ask the U.S. court for relevant protective orders to comply with EU and national data privacy rules.[185] Of course, the parties to the transcontinental litigation should find agreements to those issues before the court is approached. *TSC* suggests that the parties try to agree on suitable protective orders; those can still be applied for unilaterally in the event an agreement cannot be reached, of course.[186] Transcontinental discovery mediation is a very promising option in this regard.

However, if there is clear indication that the specific court would in a specific instance not entertain such a request, the controller should not be required to formally approach the court, as this would establish a mere dispensable formality. Adequate documentation is in order, of course, in such an instance.

The U.S. courts should be expected to support reasonable solutions, as the *U.S. Supreme Court* stressed in Aerospatiale case: „American courts, in supervising pre-trial proceedings, should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position."[187] Such a protective order might include a sealing of the file, an „attorneys-eyes-only" review process, review in camera only, and many more approaches.[188] A suitable approach has to be chosen based on the specific facts of each case.

It has to be noted that – to put it mildly – not all U.S. judges are equally willing to appreciate the needs of foreign defendants in this respect. However, proliferation of the International Principles and a heightened awareness of both legal cultures should decrease the number of oblivious judges.

In the event the U.S. court is unwilling to put the required safeguards in place, it could be further argued that Production is not permitted at all. The – relatively speaking – broad „litigation exception" with respect to litigation in foreign countries could require such a result. Safeguards that make sure that the Personal Data cannot be used outside this special purpose have to be put in place. If the court is not willing to secure those or if it is clear from the beginning that – for other reasons – the recipients of the Personal Data will not limit access to it to the legitimate purpose, the Export would then have to be enjoined. In the event the Personal Data could become accessible to the general public, the position could be taken that the data subject's overriding legitimate interests prohibit the data transfer.[189] However, in the context of Export for transcontinental litigation purposes, all fundamental rules have to be avoided. Rather, a case-by-case analysis has to be conducted. In the event the data controller has taken all steps that can be reasonably expected, the volume and

179 See Chapter VII.1.a) and VII.1.b).
180 See Chapter VII.1.c).
181 *Brisch/Laue*, RDV 2010, 1, 5; *Hanloser*, DuD 2008, 785, 787.
182 GDPR(p2012), Article 9 (f).
183 *TSC*, International Overview 2009 – Germany, p. 103.
184 *TSC*, International Overview 2009 – Germany, p. 103.
185 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 17; *Working Party*, WP 158, p. 11; *Spies/Schröder*, MMR 2008, 275, 280.
186 *TSC*, International Principles on Discovery, Disclosure & Data Protection, 2011, p. 17.
187 482 U.S. 522, 546 (No. 15, 16a).
188 *Rath/Klug*, K&R 2008, 596, 600; *Spies/Schröder*, MMR 2008, 275, 280.
189 *Spies/Schröder*, MMR 2008, 275, 279; for the contrary but not convincing view, according to which Section 26 para. 1 (d) of the Directive anticipated and solved most issues, *Hanloser*, DuD 2008, 785, 789.

specifics of the Personal Data have to be evaluated as well as the protections that the U.S. court is willing to put in place. This case-specific information then provides the basis for a decision to allow or deny the Export.

VIII. Telecommunications Privacy at the Workplace

The following chapter deals with special issues arising out of the right to telecommunication privacy and the question of its application at the workplace. Many uncertainties exist, in part resulting from the fact that a regular statute deals with the right to telecommunication privacy – Section 88 of the Telecommunications Act (Telekommunikationsgesetz, „TKG") – besides the basic right contained in Article 10 para. 1 GG. According to Section 88 para. 1 TKG, the right to telecommunications privacy comprises the content and detailed circumstances of telecommunications („Covered Telecommunication Information"). Section 88 para. 2 TKG obliges the provider of telecommunication services („Service Provider") to ensure the right to telecommunication privacy.

Neither case law nor scholars have defined the exact scope of the right to telecommunication privacy at the workplace and the resulting limitations on the employer's conduct, yet. In fact, it is even disputed that the right to telecommunication privacy exists at all at the workplace. However, the following findings represent the understanding of the authors: The employer is a Service Provider in the event private use of the Internet or the e-mail system is explicitly allowed for or at least tolerated (VIII.1). Telecommunication Information is protected within and outside of the employment context by the right to telecommunication privacy until the conclusion of the data transmission, which occurs only once the participant has exclusive control over access, copying, and forwarding of the data (VIII.2.a)). Enterprises should not assume that non-employee participants to covered telecommunication activities enjoy a lesser degree of protection (VIII.2.c)). The unauthorized Handling of Covered Telecommunication Information is prohibited by Section 88 para. 3 TKG (VIII.3) and subject to severe consequences (VIII.4). While difficult to be obtained, valid consent of all relevant participants can authorize the Handling (VIII.5.a)), albeit such consent cannot be substituted by consent of the works council (VIII.5.b)). In the event no authorization is practically or legally feasible, the employer has to ask the employee to sort through and remove all private e-mails from any given data volume. Written confirmation of the employee to that end is suggested (VIII.5.a)).

1. Employer: A Potential Provider of Telecommunication Services

The initial issue that needs to be dealt with is if the employer is a Service Provider. There is consensus that the employer is not a Service Provider if private use of the Internet and of e-mail services is expressly prohibited and not even implicitly allowed for.[190] In this case the TKG is not applicable.[191]

Unfortunately, this is where the consensus ends: Two recent decisions of high labor courts conclude that the employer is not a Service Provider, even if private use is allowed for.[192] While some scholars share this view,[193] the majority view and other court decisions reach the opposite result. Accordingly, the employer offers telecommunication services to „third parties" within the meaning of Section 3 numeral 10 TKG and qualifies as „Service Provider" in line with Section 3 numeral 6 and numeral 10 TKG in this scenario.[194] The main reason for this understanding is that the statute does neither require remuneration nor intent to make profit for the qualification of a commercial provision of telecommunication services in Section 3 numeral 10 TKG; according to the legislator, any offering of telecommunication services suffices.[195] The German supervisory authorities broadly, if not unanimously, share this view.[196]

2. End of Data Transmission

In the event the employer qualifies as a Service Provider, several uncertainties exist with respect to the scope of the right to telecommunication privacy, more specifically the question when the data transmission and therewith the protection ends. While ample decisions of the *BVerfG* exist, some scholars dispute that those are applicable in the work environment; decisions dealing with telecommunication privacy at the work place are sparse and inconsistent.

a) General Perspective

In a 2009 decision the *BVerfG* clarified the area of protection provided by the user's basic right to telecommunication privacy according to Article 10 para. 1 GG.[197] The *Court* reiterated that the basic right to telecommunication privacy does not extend to stored data once the data transmission has ended. While this was common ground, the Court went on solving a dispute as to the point in time in which the end of data transmission occurs in the case of communication via e-mail.[198]

As distant communication requires the assistance of a Service Provider and is therefore more prone to unauthorized access and interference by others, Article 10 para. 1 GG guarantees special protection to such communication. In essence, Article 10 para. 1 GG intends to provide the participants with the same level of secrecy and security than they would enjoy were they engaged in direct communication. The protection covers content and circumstances of the communication and ends only once the transmission of the data has concluded. Information stored outside of the data transmission is no longer protected by Article 10 para. 1 GG. Once the protection of Article 10 para. 1 GG ends, the user is not without protection but covered by the basic right to informational self-determination (Article 2 para. 1 GG in connection with Article 1 para. 1 GG).[199]

The end of the data transmission has to be determined based on the protection the basic right is intended to provide, not based on mere technicalities. The decisive factor is the user's ability to control access to, copying of, and forwarding of the e-mail. As long as the user lacks the respective controllability the data is still

190 In general, the decision to allow for private use lies in the sole discretion of the employer, *Altenburg/Reinersdorff/Leister*, MMR 2005, 135. Employment contracts, union contracts, company usage (betriebliche Übung), etc. can modify this result.
191 *Hoppe/Braun*, MMR 2010, 80 with further references.
192 *LAG Berlin-Brandenburg* ZD 2011, 43 m. Anm. *Tiedemann* = NZA-RR 2011, 342 ff.; *LAG Niedersachsen* NZA-RR 2010, 406 ff. = MMR 2010, 639 m. Anm. *Tiedemann*.
193 *Haussmann/Krets*, NZA 2005, 259, 261; *Wytibul*, ZD 2011, 69, 73.
194 *Junker*, Electronic Discovery gegen deutsche Unternehmen, 2008, p. 83; *Hoppe/Braun*, MMR 2010, 80, 81; *Altenburg/Reinersdorff/Leister*, MMR 2005, 135, 136; Anm. *Tiedemann*, ZD 2011, 45, 46; Taeger/Gabel/*Munz*, BDSG, Section 88 TKG, marginal 20; Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, Section 88 TKG, marginal 18; *Rath/Klug*, K&R 2008, 596, 598; *Hanloser*, DuD 2008, 785, 787, 788; *Härting*, Internetrecht, 4. Edition 2010, marginal 130 f.; *Hoeren*, online script „Internetrecht" Stand: April 2011, p. 396, available under: http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/lehre/lehrematerialien.htm; *Polenz/Thomsen*, DuD 2010, 614; *Schmidl*, MMR 2005, 343, 344; Simitis/*Seifert*, BDSG, 7. Edition 2011, Section 32, marginal 92; *LAG Berlin-Brandenburg* ZD 2011, 43 m. Anm. *Tiedemann* = NZA-RR 2011, 342 ff.; *Brink*, in: jurisPR-Arbeitsrecht, annotation on *LAG Berlin-Brandenburg*; *OLG Karlsruhe* DuD 2005, 167 ff = MMR 2005, 178 m. Anm. *Heidrich*; *ArbG Hannover* NZA-RR 2005, 420, 421.
195 BT-Drs. 13/3609, p. 53 (document of the German Bundestag).
196 *Federal Commissioner for Data Protection and Freedom of Information*, "Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz", January 2008, available under: http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenInternetAmArbeitsplatzneu.pdf?__blob=publicationFile.
197 *BVerfG* MMR 2009, 673 ff. m. Anm. *Krüger*.
198 The diverse opinions are set forth by Anm. *Krüger*, MMR 2009, 680, 681.
199 *BVerfG* NJW 2006, 976, 978.

protected by the right to telecommunication privacy and Covered Telecommunication Information continues to exist. While prior decisions of the *BVerfG*, inter alia a decision from 2006,[200] indicated a different view, the actual controllability in the specific situation has to be evaluated. Hence, it does not matter, if the user could have saved the e-mail in a way to ensure exclusive controllability, if he actually did not in a specific situation.[201] The *BVerfG* did not leave any doubt in its fundamental ruling, as even the critics have to admit.[202]

In the case decided by the *BVerfG*, a user had used IMAP and the e-mails remained stored on the Service Provider's server. As the Service Provider still had access – and the user consequently lacked exclusive controllability with respect to access, copying and forwarding – the data transmission had not ended and the user was still protected by the basic right to telecommunication privacy.[203] This result was reached irrespective of the fact that the user protected his e-mails with a password and that he did not make use of the existing possibility to remove the e-mails from the server.

Other additional factors considered by the *BVerfG* favor the result that e-mails stored on the Service Provider's server continue to constitute Covered Telecommunication Information: The Service Provider is still involved in the administration of the e-mail.[204] Given the actual lack of exclusive controllability, the user is not able to establish mechanisms to exclude third party access to the Telecommunication Data.[205] The risk of covert access to the Telecommunication Data still exists. While such risk is not constitutive, it is typical and increases the weight of possible infringements of the right to telecommunication privacy.[206] From an overall perspective the Telecommunication Information is not just subject to the possibility of access by third parties to the extent any other data created or stored by the user is; to the contrary, a specific transmission related risk exists with respect to which the right to telecommunication privacy provides protection. This protection stays in effect as long as an e-mail is stored on the server of the Service Provider.

b) Employee Perspective

Conflicting views on the issue exist with respect to the question if the above-stated ruling of the *BVerfG* applies at the workplace, at all. While there are no affirmative court decisions on point – post-dating the 2009 ruling – available, most scholars believe that this is the case.[207] Most of those opine, that workplace e-mails are covered by the employee's basic right to telecommunication privacy, if private use is explicitly allowed for or tolerated and as long as the employer has still non-restrictable access. It is suggested that this holds true even if the employer has access to those e-mails only via backup tapes of the e-mail system.[208] However, once the employee saves the e-mails exclusively outside of the e-mail system, even if they are still accessible by the employer (e.g., if saved on a corporate server), the transmission and consequently the protection ends.

The opposite view disputes that the decision of the *BVerfG* is applicable at the workplace at all, as it concerns only the basic right to telecommunication privacy as set forth in the GG and not the one set forth in the regular statute, Section 88 TKG more specifically. According to this view, Article 10 para. 1 GG is directly applicable only with respect to governmental authorities, while enterprises are solely regulated by Section 88 TKG, and the TKG does not extend to dormant communication, as, according to Section 3 numeral 22 TKG, the "telecommunication" term of the TKG seems to imply a "dynamic" process.[209]

An intermediary view opines that the right to telecommunication privacy protects employees in general, but that the protection ends at the time of sending or receiving e-mails, provided that the employee has the exclusive abstract power to keep or remove the e-mail from the e-mail system. In the event the e-mail is kept in the employer's e-mail system after a legitimate possibility exits to remove it from there for the employee, there is no longer any need to protect the employee.[210]

Neither the opposite nor the intermediate view is in line with the fundamental ruling of the *BVerfG* from 2009. The protection of Telecommunication Information is required as long as the e-mail is stored on the server of the Service Provider and the user lacks the ability to restrict access of the Service Provider or any third party. In addition, the *BVerfG* expressly rejected the relevance of the abstract user's ability to remove the e-mail form the server, if – in the specific situation – such removal did not occur. As the decision of the *BVerfG* expresses a fundamental view on the protection required by Article 10 para. 1 GG, the better arguments speak for the understanding that the regular statute, Section 88 TKG, has to be viewed in the light of the basic right as interpreted by the *BVerfG*.[211]

Therefore, the data transmission and herewith the protection ends only once the employee's e-mail is removed from the employer's e-mail system entirely and no possibility of reconstruction exists.

c) Third Party Perspective

The equation gets even more complex, if a third party is added. The right to telecommunication privacy in general protects all participants to a telecommunication activity;[212] with respect to communication via e-mail the sender and (all) recipients. Therefore, authorization of the employee and of at least one non-employee participant would be required in the event of e-mail communication with anyone outside of the employment relationship.[213]

Some scholars argue that the protection of the right to telecommunication privacy ends for the sender once the e-mail is received by the server of the recipient, respectively the server of his employer, negating the need for authorization by the third party sender of an e-mail.[214] Those scholars reference the 2006 decision of the *BVerfG*, according to which the data transmission ends, once the e-mail is received and a possibility to remove the e-mail from the e-mail system exits.[215] They argue, that – from a „traditional perspective" – dormant communication is not covered by the right for telecommunication privacy.[216] In addition,

200 *BVerfG* NJW 2006, 976, 978 = MMR 2007, 217.
201 *BVerfG* MMR 2009, 673, 674 m. Anm. *Krüger*.
202 *Krüger*, MMR 2009, 680, 681 m. Anm. *Krüger*.
203 *BVerfG* MMR 2009, 673, 675 m. Anm. *Krüger*.
204 *BVerfG* MMR 2009, 673, 675 = MMR 2006, 217.
205 *BVerfG* NJW 2006, 976, 978.
206 *BVerfG* NJW 2006, 976, 978, 981 = MMR 2006, 217; *BVerfG* MMR 2009, 673, 677 m. Anm. *Krüger*.
207 *Hoppe/Braun*, MMR 2010, 80, 82; along the same line *Panzer-Heemeier*, DuD 2012, 48, 52; Anm. *Tiedemann*, ZD 2011, 45, 46.
208 *Hoppe/Braun*, MMR 2010, 80, 82; along the same line *de Wolf*, NZA 2010, 1206, 1209.
209 *Behling*, BB 2012, 892, 894; *Härting*, Internetrecht, marginal 116, 140.
210 *Panzer-Heemeier*, DuD 2012, 48,52; Anm. *Tiedemann*, ZD 2011, 45, 46; probably along the same line Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, Section 88 TKG, marginal 32; *VGH Kassel* NJW 2009, 2470 ff. = MMR 2009, 714.
211 This holds true even if the *BVerfG* stated that the scope of the basic right can exceed the right according to Section 88 TKG (*BVerfG* MMR 2009, 673 ff. = MMR 2009, 714.).
212 BVerfGE 85, 386, 399; Spindler/Schuster/*Eckhardt*, Recht der elektronischen Medien, Section 88 TKG, marginal 14, 15; *Schmidl*, MMR 2005, 343, 346.
213 *Polenz/Thomsen*, DuD 2012, 614, 615.
214 *Kempermann*, ZD 2012, 12, 14; *Haussmann/Krets*, NZA 2005, 259, 261; in the same vein, but with respect to filtering for spam-e-mails *Sassenberg/Lammer*, DuD 2008, 461, 462.
215 *BVerfG* NJW 2006, 976 ff = MMR 2006, 217; following this decision *VGH Kassel* NJW 2009, 2470 ff. = MMR 2009, 714.
216 *Kempermann*, ZD 2012, 12, 14.

as the sender of an e-mail has no control over the handling by the recipient – whether he deletes it, saves it inside of the e-mail system or outside of it in a way that the protection of the right to telecommunication privacy ends – he is not entitled to the respective protection, once the e-mail is received. Another argument denying the need for protection can be evolved around the thought that the sender of an e-mail to a corporate account has, in most cases, no information about the recipients e-mail policies and accordingly no expectation of coverage.

While all of those arguments bear some weight, it is hard to predict how German courts would rule on this specific issue and detailed scholarly opinions are sparse. Moreover, the 2009 decision of the *BVerfG* indicates a different and rather expansive interpretation of the right to telecommunication privacy. In addition, the *BVerfG* did not state that the extension of the coverage with respect to dormant communication is limited to the recipient only, excluding the sender. Over and above, in the event the employee is the sender of the e-mail, the employer has no information whatsoever, if the respective e-mail is still covered by the recipient's right to telecommunication privacy, at all. Therefore, enterprises should not operate on the assumption that consent of a (non-employee) third party sender or recipient is not necessary, provided they deal with Covered Telecommunication Information.

3. General Prohibition to Procure Telecommunication Information

Insofar as information is protected by telecommunication privacy, Section 88 para. 3 TKG enjoins the employer from obtaining for himself or for other parties beyond what is necessary for the commercial provision of the telecommunications services. Knowledge of any Covered Telecommunication Information may only be used for this specific purpose. Clearly, any information collected for general business litigation purposes does not fall within this category. Any use for other purposes, in particular, passing it on to other parties, is permitted only insofar as provided for by the TKG or any other legal provision that makes reference to telecommunications activities explicitly (Section 88 para. 3 sentence 3 TKG).

Analyzing the legislative rationale behind the TKG exemplifies this further and highlights the weight that is put on the respective right. In the event of a (national) governmental intervention law or a governmental right to demand information that would interfere with the basic right to telecommunication privacy, the governmental law or right only trumps the basic right provided the statute explicitly references telecommunication activities and provided legislative intent is documented favoring governmental intervention over the basic right. Statutes establishing general obligations to provide information without such reference and without the documented legislative intent cannot legitimize interventions with respect to the right to telecommunication privacy.[217] Therefore, if the tax authorities would inquire into Covered Telecommunication Information of a financial institution – based on the governmental right to demand information from third parties that are relevant for taxation purposes of a customer as set forth in Section 93 Abgabenordnung (Fiscal Code, „AO") – the financial institution could not provide such information, as Section 93 AO does not explicitly reference telecommunication activities. *Hoppe/Braun* describe a fact pattern that involves the *SEC*: Based on a request from the *SEC* relating to an insider dealings matter, the *Federal Financial Supervisory Authority* in Germany asked a company to provide e-mails that were sent to or received by certain employees. The statutory basis for the request (Section 7 para. 7 in connection with Section 4 para. 3 WpHG (Securities Trading Act)) only states that the national authority may request certain information and documents from everybody. As the statutory basis does not specifically refer to telecommunication activities the company cannot comply with the request without violating the TKG.[218]

No provision of the German or European law meets the requirements with respect to collecting or using Covered Telecommunication Information for general business litigation pending in the U.S. Compliance with the rules of civil procedure of a foreign country or the order of a court of a foreign country cannot justify the violation of the right to telecommunication privacy, either. Justifications, which arguably allow such intrusions to avoid harm, e.g. suspicion of criminal activity, suspicion of divulging of trade secrets, etc.,[219] are not applicable in this regard.[220]

Therefore, if one assumes that the right to telecommunication privacy applies at the workplace in the event private use is allowed for or tolerated and that dormant communication is covered as well, the employer cannot monitor or control Telecommunication Data absent authorization. In addition, even the screening, e.g. using key word searches, of such data likely already violates Section 88 para. 3 TKG.[221]

In the event that private e-mails are not unequivocally severable from business e-mails, the business related e-mails have to be treated as private e-mails. Insofar, the private classification infects the business e-mails. The reasoning behind this approach is that the employer cannot examine or sort all e-mails arguing that he will examine only the business e-mails further. The distinction between private and business e-mails has to be made prior to each step in the Handling chain. Even flagging by the employee of e-mails as „private" does not solve the problem, as incoming private e-mail will in most instances not be compliant with the flagging requirement.[222]

4. Consequences of Violation of Telecommunication Privacy

At least any unauthorized further transfer to a third party of Covered Telecommunication Information constitutes a criminal activity according to Section 206 para. 1 Strafgesetzbuch (Criminal Code, „StGB"). The prohibition of such transfer applies to owners and employees of Service Providers.

In the event Covered Telecommunication Information is transferred – even if only to the enterprise's outside counsel, be it in Germany, Europe or abroad – an actual risk of criminality exist, absent authorization.[223] The same is true for such transfers to opposing counsel, third parties, and the U.S. court, of course. Even if such data is solely provided to other employees, such as in-house counsels or in-house experts, criminality cannot be excluded. According to the wording of the statute, any unauthorized transfer to a third party, including other employees, can cause criminality.[224]

Provided covered data is merely obtained unlawfully without any transfer to a third party, Section 206 StGB is not applicable.

217 BT-Drs. 13/3609, p. 53 (document of the German Bundestag), with respect to the (identical) previous version of Section 82 para. 3 TKG.
218 *Hoppe/Braun*, MMR 2010, 80, 83.
219 According to *Hoppe/Braun*, MMR 2010, 80, 81, the existence of such an exception is widely presumed, duly reflecting the conflicting interests but disparate with the wording of the statute.
220 *Hanloser*, DuD 2008, 785, 787 f. with further reference.
221 *Hoppe/Braun*, MMR 2010, 80, 81; *Hanloser*, DuD 2008, 785, 787.
222 *Hoppe/Braun*, MMR 2010, 80, 83; *Koch*, NZA 2008, 911, 913; *Vietmeyer/Beyers*, MMR 2010, 807, 809.
223 A further detailed analysis of potential criminal justifications lies outside of the scope of this publication.
224 A detailed analysis of this issue lies outside of the scope of this publication.

However, the covered data will in most instances contain Personal Data, as defined above,[225] and collecting Personal Data can constitute a regulatory offence,[226] which would be punishable with a fine of up to € 300.000,– .[227]

5. Valid Authorization

In light of the severe consequences, especially the risk of criminality, of a violation of the right to telecommunication privacy as set forth in Section 88 para. 3 TKG, enterprises are well advised assuming that Covered Telecommunication Information cannot be legally handled or transferred to the U.S. without authorization.[228] This is in line with the finding of *TSC*, which states that an area of „private" communication (private e-mails) exists that is protected by the law, in particular Section 88 TKG. In the words of *TSC*: „This 'private communication' would probably not be discoverable" unless authorized.[229]

a) Consent of the Relevant Participants

Given the high risk, employers seek ways to legitimize their Handling of Covered Telecommunication Information. In the event valid consent exists, criminality with respect to Section 206 para. 1 StGB is eliminated due to a lack of the required criterion „unauthorized".

Insofar as consent of the relevant participants is required,[230] the statute mandates no specific form. In other words, consent can be included in the employment contract, a separate declaration of the employee, given orally,[231] or even implicitly. A union contract can provide that private use is allowed for only, if valid consent of the individual employee exists and that such consent is provided implicitly once the employee uses the Internet or the e-mail system for private use.

However, only if the information provided allows the employee to assess the coverage of the consent,[232] can the consent be considered valid.[233] Proper information requires that it is clearly stated that the employee's right to telecommunication privacy maybe infringed upon for reasons of compliance with U.S. discovery obligations. In addition, it is suggested that the information sets forth that all kinds of ESI can be concerned and that the potential recipients of the Telecommunication Information (in-house and external counsel and experts, litigation service providers, parties to the litigation, U.S. courts) are mentioned.

If all forms of authorization by means of consent fail, the employer has – as a means of last resort – to ask the employee to sort through and remove all private e-mails before the employer can handle the information further.[234]

b) Involvement of the Works Council

TSC states that either the individual or the works council of the company can consent and authorize the Handling.[235] This is at least misleading: Even if one would only require the employee's consent – and not the consent of non-employee participants – the works council's consent could not substitute the individual employee's consent. The TKG, other than Section 4 para. 1 BDSG, does not contain a savings clause that would allow for collective bargaining agreements („Tarifvertrag") or union contracts,[236] which would have a negative impact on the individual employee's right to telecommunication privacy. Therefore, those regulations cannot authorize infringements of the right to telecommunication privacy.

However, if a policy for the Handling of work-related Covered Telecommunication Information is to be implemented and a works council exists, the works council has to be involved. It has broad co-determination rights with respect to the introduction and use of technical devices designed to monitor the behavior or performance of the employees according to Section 87 para. 1 numeral 6 Betriebsverfassungsgesetz (Employees' Representation Act, „BetrVG").[237] Therefore, scholars suggest including a provision in the respective union contract, according to which the right to telecommunication privacy can be infringed in line with precisely mentioned rules and – of course – irrespective of the required individual employee's consent.[238]

IX. Final Results

A conflict exists between the U.S. rules of civil procedure, more specifically conventional and electronic discovery, and the basic right to data privacy in the E.U. and Germany. The GDPR(p2012) will not ease that conflict (Chapter I and II).

The BDSG allows the Handling of Personal Data only if permitted by the BDSG itself, another German or European law, or if the data subject provided valid consent in advance. Each step in the Handling chain has to be evaluated separately and requires specific permission. All general and specific options to legitimize the Handling of Personal Data are subject to the paramount principles of data reduction and data economy (Chapter II).

Export of Personal Data for purposes of transcontinental litigation requires a two-step evaluation, as valid consent of all required data subjects will hardly ever be obtainable; be it for practical or legal reasons. Legitimization from a general as well as an Export specific perspective is required. Safeguarding the data controller's legitimate interest forms the general basis with respect to Section 28 BDSG, while „necessity related to legal claims" forms the specific basis with respect to Section 4b, 4c BDSG respectively. A Balancing Test is already required on the first level to ensure proportionality; an Export Balancing Test has to be passed in addition to allow for the transfer of Personal Data to a third country. With respect to the later one, the scale tips on the side of non-Export initially, as the Export is disfavored (Chapter III).

Applying the principles and basic rules set forth in Chapter III, the following generalized guideline is provided with respect to each step in the Handling chain:

Preservation, including the creation of a backup tape, of the Preserved Data is legitimate to the extent required by the lex fori (Chapter IV). No general additional requirements are posted during the phase of Internal Review (Chapter V).

---

225 See Chapter II.4.
226 Section 43 para. 2 numeral 1 BDSG. The e-mail content does not represent customer or traffic data within the meaning of Section 3 numeral 3 and numeral 30 TKG with the consequence that not the data privacy norms of the TKG (Section 91 ff. TKG) but those of the BDSG are applicable.
227 Section 43 para. 3 BDSG.
228 *Rath/Klug*, K&R 2008, 596, 598 f.
229 *TSC*, International Overview 2009 – Germany, p. 100.
230 With respect to the question of the actual required consentees, see Chapter VIII.2.
231 For evidentiary reasons formless consent is not recommended, however.
232 *Gola/Wronka*, Handbuch zum Arbeitnehmerdatenschutz, 5. Edition 2010, marginal 1827.
233 Written notice of receipt with respect to the information is suggested for evidentiary reasons; Progress Report of the Bavarian Supervisory Authority for the non-public Sector (Government of Central Franconia) 2002/2003, p. 54, available under: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/dsa_Taetigkeitsbericht2002-2003.pdf.
234 *Hanloser*, DuD 2008, 785, 788.
235 *TSC*, International Overview 2009 – Germany, p. 100.
236 *Altenburg/Reinersdorff/Leister*, MMR 2005, 222, 223; *Haussmann/Krets*, NZA 2005, 259, 263; *Hoeren*, online script „Internetrecht" Stand: April 2011, p. 396, available under: http://www.uni-muenster.de/Jura.itm/hoeren/INHALTE/lehre/lehrematerialien.htm.
237 Simitis/*Seifert*, BDSG, 7. Edition 2011, Section 32, marginal 94; *Rath/Klug*, K&R 2008, 596, 599; *Spies*, MMR 7/2007, p. V, VII; *Haussmann/Krets*, NZA 2005, 259; *Däubler*, Gläserne Belegschaften, 5. Edition 2010, marginal 833.
238 *Pröpper/Römermann*, MMR 2008, 514, 517; *Polenz/Thomsen*, DuD 2010, 614, 616; *Haussmann/Krets*, NZA 2005, 259, 261.

Litigation, within or outside the E.U., usually requires extensive external review of Personal Data by outside counsel, non-legal service providers, and experts. On the general level such Handling will most likely be legitimate as it is necessary with respect to a proper defense against a legal claim (Chapter VI.1). Prior to the Export of Personal Data, however, all reasonably culling has to be performed, the Personal Data be anonymized or pseudonymized, and the data subjects informed properly to the extent reasonable (Chapter VI.2).

Production of Personal Data may only occur, after the utmost care is given to final culling, anonymization, and pseudonymization. Moreover, suitable court orders with respect to discovery and protective orders have to be sought (Chapter VII).

With respect to telecommunications law at the workplace it was found that the employer is a Service Provider in the event private use of the Internet or the e-mail system is allowed for or tolerated. Once the employer qualifies as Service Provider, the related Telecommunication Information is protected by the right to telecommunication privacy until the conclusion of the data transmission. This conclusions occurs – within and outside of the employment context – only once the participant has exclusive control. The unauthorized Handling of Covered Telecommunication Information subjects the Service Provider and its employees to severe consequences. While difficult to be obtained, valid consent of all relevant participants can authorize the Handling. Collective consent cannot authorize the Handling, however. In the event no authorization is practically or legally feasible, the employee has to separate the business from the private e-mails (Chapter VIII).

Dr. Ralf Deutlmoser, LL.M. (Alabama)
practices as attorney at law and mediator in Munich. He is admitted to the bar in Germany and U.S. (New York).

Alexander Filip
Head of the Department "International Data Transfers, Trade, Commerce, Industry" at the Data Protection Authority for the Privated Sector of Bavaria (Bayerisches Landesamt für Datenschutzaufsicht, Ansbach). The present text represents solely his personal opinion.

Datenschutz im Fokus.

ZD – Die neue Zeitschrift bei C.H.BECK

Die ZD informiert umfassend über datenschutzrechtliche Aspekte aus allen Rechtsgebieten. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B.
■ Konzerndatenschutz ■ Beschäftigtendatenschutz ■ Datenschutzaudit ■ Compliance ■ Einwilligung ■ Kundendatenschutz ■ Adresshandel ■ Telekommunikation ■ Soziale Netzwerke ■ Vorratsdatenspeicherung ■ Datentransfer in Drittstaaaten.

ZD – die praktischen Seiten des Datenschutzes

Jedes Heft enthält ein Editorial, fundierte Aufsätze mit praxisorientierten Lösungsvorschlägen, Abstracts durchgehend in Deutsch und Englisch, Leitworte und Schlagwortketten zur **schnellen Einordnung,** aktuelle Gerichtsentscheidungen mit Anmerkungen, aktuelle Meldungen.

Die Homepage der ZD mit weiteren Informationen finden Sie unter **www.zd-beck.de.**

3 Hefte gratis

bestellen Sie das kostenlose Schnupperabo unter www.beck-shop.de/9002683.

Bestellen Sie bei Ihrem Buchhändler oder bei:
beck-shop.de oder Verlag C.H.BECK · 80791 München · **Fax: 089/38189-402** · www.beck.de

C.H.BECK

Preis inkl. MwSt./158812

MMR – Sachverstand und Fachwissen.

MMR: Überblick und Praxisnutzen garantiert.

MMR informiert umfassend über alle Bereiche des Informations-, Telekommunikations- und Medienrechts. Die einzelnen Rubriken garantieren einen schnellen Überblick und eine hervorragende Lesbarkeit:
■ eCommerce ■ IT-Vertragsrecht ■ Immaterialgüterrecht ■ Wettbewerbs- und Kennzeichenrecht ■ Telekommunikations- und Medienrecht

Außerdem: Zahlreiche **Urteilsanmerkungen, Leitsätze** zur weiterführenden Rechtsprechung im eigenen **Leitsatzdienst** mehrmals im Jahr und MMR-FOKUS mit **ausgewählten Autoren-Beiträgen**.

Zusätzlich: Newsdienst MMR-Aktuell inklusive

Profitieren Sie zweimal im Monat von dem **E-Mail-Dienst** mit Nachrichten und aktuellen Meldungen zum Multimediarecht – ohne weitere Kosten.

Die Homepage der MMR mit weiteren Informationen finden Sie unter **www.mmr.de**

3 Hefte gratis

bestellen Sie das kostenlose Schnupperabo unter www.-beck-shop.de/1584.

Bestellen Sie bei Ihrem Buchhändler oder bei:
beck-shop.de oder Verlag C.H.BECK · 80791 München · **Fax: 089/38189-402** · www.beck.de

C.H.BECK

Preis inkl. MwSt./141405