



Datentransfer im Konzern

BESCHÄFTIGTENDATENSCHUTZ Der Transfer von Arbeitnehmerdaten im Konzern ist in Zeiten der Zentralisierung von Aufgaben und Social Intranets für die Interessenvertretung eine große Herausforderung. Doch Betriebsvereinbarungen und zusätzliche vertragliche Regelungen helfen beim weltweiten Schutz von Mitarbeiterdaten.

VON BRUNO SCHIERBAUM

Das Datenschutzrecht stellt bereits Einzelunternehmen vor große Herausforderungen. Aber zunehmend gliedern Unternehmen Bereiche als eigenständige Unternehmen aus. Auch sind Unternehmen in Konzernverhältnisse eingebunden, mit einer Vielzahl von Firmen, die ihrerseits ihren Sitz in Deutschland, in einem Land der Europäischen Union oder des Europäischen Wirtschaftsraums (EWR) oder aber in anderen Ländern außerhalb Europas – sogenannten Drittländern – haben.

Konzerne werden oftmals zentral geführt, so dass ein stetiger Datenfluss zwischen den einzelnen Unternehmen stattfindet.¹ Dieser Datenfluss kann zum Beispiel durch eine

Zentralisierung der IT-Abteilung oder der Personalverwaltung gegeben sein.² Damit einher geht die Einrichtung von konzernweit nutzbaren Kunden- und Personaldatenbanken. Auch die konzernweite Nutzung eines Intranets mit personenbezogenen Daten der Beschäftigten, wie einem Telefonverzeichnis oder E-Mail-Adressen aller Beschäftigten der Konzernunternehmen ist gängige Praxis.³

Da sich das Bundesdatenschutzgesetz (BDSG) an das einzelne Unternehmen richtet, gibt es keine Privilegierung des Datentransfers zwischen einzelnen Unternehmen eines Konzerns. Der Datentransfer unterliegt diesem Gesetz, das auch bei Unternehmen zu beachten ist, die nicht im Konzernverbund sind.

¹ Vgl. v. d. Bussche / Voigt, Einführung und Checkliste, in: v. d. Bussche / Voigt, Konzerndatenschutz, 1

² Siehe Moos / Zeiter, Konzerndatenschutz, in: Forgo / Helfrich / Schneider (Hrsg.), Betrieblicher Datenschutz, 328 f.

³ Vgl. Hoeren, Das Konzerntelefonverzeichnis – ein datenschutzrechtlicher Sündenpfuhl?, in: ZD 9/2014, 441 f.

Kein »Konzernprivileg«

Beim Datenschutz im Konzern ist zu beachten, dass sich das BDSG an nicht-öffentliche Stellen wendet. Das sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, § 2 Abs. 3 BDSG. Maßgeblich ist erst einmal die privatrechtliche Organisationsform. Natürliche Personen, etwa in Ausübung einer selbstständigen Tätigkeit sowie alle privatrechtlich organisierten Unternehmungen und Vereinigungen (GmbH, OHG, KG, Verein, Stiftung oder etwa Partei) gehören hierzu. Für die Einhaltung und Umsetzung des BDSG ist in erster Linie das einzelne Unternehmen und der Geschäftsführer verantwortlich und nicht der einzelne Betrieb oder der Konzern.⁴

Rechtmäßige Datentransfers

Sollen personenbezogene Daten von einem Unternehmen an ein anderes Unternehmen innerhalb oder auch außerhalb eines Konzerns transferiert werden, ist dieses vorher datenschutzrechtlich zu prüfen. Grundsätzlich ist es für das einzelne Unternehmen oder für den Konzern von zentraler Bedeutung, die Datenströme zwischen den einzelnen Unternehmen zu analysieren, um die Verantwortlichkeit für eine Verarbeitung, Übermittlung oder Nutzung personenbezogener Daten festzustellen.⁵

Auf dieser Basis ist die rechtmäßige Datenverarbeitung beziehungsweise der rechtmäßige Datentransfer zu prüfen. Es gibt im BDSG zwei Möglichkeiten, rechtmäßig Daten von einem Unternehmen zu einem anderen zu transferieren.

Zum einen kann eine Übermittlung personenbezogener Daten vorliegen. Das Unternehmen, an das Daten übermittelt werden sollen, ist Dritter im Sinne des BDSG. Ein Übermitteln personenbezogener Daten kann das Bekanntgeben gespeicherter personenbezogener Daten an einen Dritten in der Weise sein, dass die Daten an ihn weitergegeben werden oder er zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen, § 3 Abs. 4 Nr. 3 BDSG. Von datenschutzrechtlicher Bedeutung ist beim Übermitteln von Daten nicht nur das aktive Zusenden personenbezogener Daten von einem Unternehmen an ein anderes. Übermittlung liegt auch dann vor, wenn ein Unternehmen eigenständig auf Datenbanken

zugreift, die von einem anderen (Mutter- oder Tochter-)Unternehmen lediglich für andere bereitgehalten werden.⁶ Das Übermitteln von personenbezogenen Daten unterliegt dem sogenannten Verbot mit Erlaubnisvorbehalt gemäß § 4 Abs. 1 BDSG.

Zum anderen kann ein Datentransfer von einem zu einem anderen Unternehmen im Rahmen von Auftragsdatenverarbeitung gemäß § 11 BDSG stattfinden. Es liegt dann keine Übermittlung personenbezogener Daten vor. Denn die gesetzliche Konstruktion der Auftragsdatenverarbeitung basiert auf der Bestimmung des § 3 Abs. 8 BDSG. Danach sind Personen und Stellen, die im Geltungsbereich des BDSG, in der EU oder im EWR personenbezogene Daten im Auftrag verarbeiten, nicht Dritte.⁷ Auftragsdatenverarbeitung stellt somit ein Privileg da. Der Datentransfer muss nicht gemäß § 4 BDSG legitimiert werden, sondern durch einen Vertrag gemäß § 11 BDSG. Dieses Privileg gilt dann nicht, wenn personenbezogene Daten in ein Drittland – also in ein Land außerhalb der EU oder des EWR – transferiert werden sollen. Das kann ausschließlich auf der Basis des § 4 in Verbindung mit § 32 BDSG erfolgen, wobei zusätzlich in dem Drittland – genauer gesagt in dem Unternehmen im Drittland – ein »angemessenes Datenschutzniveau« gegeben sein muss.

Übermitteln von Beschäftigtendaten

Die Zulässigkeit der Erhebung, Verarbeitung – wozu auch die Übermittlung zählt – und Nutzung personenbezogener Daten im Rahmen von Beschäftigungsverhältnissen bestimmt sich nach § 4 in Verbindung mit § 32 BDSG. Nach § 4 BDSG ist die Verwendung personenbezogener Daten nur zulässig, soweit das BDSG (§ 32 beim Arbeitnehmerdatenschutz) selbst oder eine andere Rechtsvorschrift dieses vorsieht oder erlaubt oder der Beschäftigte eingewilligt hat.

Die zentrale Vorschrift bildet der § 32 BDSG, wonach eine Übermittlung für die Durchführung des Beschäftigtenverhältnisses erforderlich sein muss. Hierauf eine Übermittlung personenbezogener Daten von einem Unternehmen zu einem anderen (innerhalb eines Konzerns) zu stützen ist zwar strittig, unter Datenschützern aber wohl auszuschließen.⁸

Alternativ kann der Arbeitgeber auch mit Einwilligung der Beschäftigten arbeiten, dabei

DARUM GEHT ES

1. Der Datentransfer im Konzern bedarf immer einer Rechtsgrundlage.
2. Der Schutz der Beschäftigtendaten ist überall zu gewährleisten.
3. Betriebliche Vereinbarungen können den Datentransfer rechtfertigen – und Arbeitnehmerdaten schützen.

4 Siehe Gola / Schomerus, BDSG, § 2 Rn. 19 ff.

5 Vgl. Hoeren, EU-Standardvertragsklauseln, BCR und Safe Harbor Principles, in: RDV 6/2012, 272

6 Hoeren, EU-Standardvertragsklauseln, BCR und Safe Harbor Principles, aaO., 271

7 Vgl. Gola / Schomerus, aaO., § 11 Rn. 3

8 Vgl. Wedde, Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats, in: v.d. Bussche / Voigt, Konzerndatenschutz, 174 f.

LITERATURTIPP

Zur Auftragsdatenverarbeitung in der neuen EU-Datenschutzgrundverordnung siehe:

Jochen Brandt, EU-Datenschutz – fünf zentrale Punkte,

in: CuA 3/2016, 17 ff.

entsteht aber für den Arbeitgeber ein Problem, wenn der Beschäftigte seine einmal erteilte Einwilligung widerruft. Das heißt, die Möglichkeit der Einwilligung ist für eine langfristige Übermittlung von Beschäftigtendaten von vornherein mit durchgreifenden Bedenken verbunden.⁹

Betriebliche Vereinbarung

Als tragbarer Weg für eine rechtmäßige Übermittlung kann der Abschluss einer Betriebsvereinbarung dienen. Im Rahmen der Vorgaben des BetrVG und des BDSG können die Betriebsparteien Datenverarbeitungsprozesse gestalten. Grundsätzlich können durch betriebliche Vereinbarungen auch Datenübermittlungen innerhalb eines Konzerns gerechtfertigt werden.¹⁰ Das ist natürlich nur möglich, wenn es einen Betriebsrat beziehungsweise einen Gesamt- oder Konzernbetriebsrat (GBR/KBR) gibt.

Beim Einsatz von IT-Systemen ist das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG anzuwenden, denn es liegt die Einführung und/oder Anwendung einer technischen Einrichtungen vor, die dazu bestimmt ist, die Leistung oder das Verhalten der Beschäftigten zu überwachen. Um dieses Recht auszulösen, genügt es, wenn das technische System objektiv geeignet ist, Leistung oder Verhalten zu überwachen. Die Mitbestimmung kommt auch dann zum Tragen, wenn entsprechende technische Systeme nicht durch den Arbeitgeber selbst, sondern durch ein anderes Unternehmen betrieben werden. Denn auch in dieser Hinsicht besteht kein Konzernprivileg. Verantwortliche Stelle ist und bleibt der Arbeitgeber.¹¹

▶ **Zuständige Interessenvertretung**

Ob der örtliche Betriebsrat, der GBR oder KBR zuständig ist, gibt das BetrVG vor.¹² Es stellt darauf ab, dass die Mitbestimmungsrechte vorrangig vom Betriebsrat wahrgenommen werden. Die Zuständigkeit des GBR oder KBR sind dann originär gegeben, wenn es sich um eine Angelegenheit handelt, die mehrere Betriebe oder mehrere Unternehmen betreffen und nicht innerhalb des Einzelbetriebs regelbar sind, § 50 und § 58 BetrVG. Beide Voraus-

setzungen müssen gegeben sein. Die originäre Zuständigkeit des GBR oder KBR setzt eine objektive Unmöglichkeit des Betriebsrats beziehungsweise des GBR voraus, die Angelegenheit regeln zu können. Werden (Gesamt-) Betriebsvereinbarungen abgeschlossen, ist vertraglich zwischen den Unternehmen im Konzern sicherzustellen, dass die betrieblichen Vereinbarungen in den anderen Konzernunternehmen zur Anwendung kommen.

Eine Konzernbetriebsvereinbarung findet Anwendung auf alle Konzernunternehmen in Deutschland und erstreckt sich auch auf Unternehmen, die keinen GBR gebildet haben sowie auf Betriebe ohne Betriebsrat. Der Abschluss von Vereinbarungen ist auch dann nachdrücklich zu empfehlen, wenn Datenverarbeitung im Auftrag vorliegt.

Datenverarbeitung im Auftrag

Die zweite Möglichkeit, rechtmäßig personenbezogene Daten innerhalb von Konzernen zu transferieren, ist die Auftragsdatenverarbeitung gemäß § 11 BDSG. Datenschutzrechtlich ist der Auftragnehmer nicht »Dritter«, sofern er seinen Sitz innerhalb der EU oder des EWR hat. Insoweit könnte der Auftragnehmer mit der Rechtsform einer französischen Aktiengesellschaft für deutsche Unternehmen personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen. Das heißt, die Datenverarbeitung im Auftrag bietet eine erhebliche Privilegierung der Auslagerung von IT-Tätigkeiten.¹³

Es liegt bei ihr kein »Übermitteln« personenbezogener Daten vor, so dass im Vorfeld eine Zulässigkeitsprüfung nicht erforderlich ist. Es ist aber ein Vertrag zum Schutz der personenbezogenen Beschäftigtendaten abzuschließen, durch den sicherzustellen ist, dass der Auftraggeber datenschutzrechtlich verantwortlich bleibt und gegenüber dem Auftragnehmer weisungsbefugt ist.

Der Auftragnehmer ist »Herr der Daten« und bleibt vollständig für den Datenschutz verantwortlich. Das beauftragende Unternehmen hat sich vor Beginn der Verarbeitung personenbezogener Daten und sodann regelmäßig von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen nach § 9 BDSG zu überzeugen. Das Ergebnis

9 Hoeren, EU-Standardvertragsklauseln, BCR und Safe Harbor Principles, aaO., 273

10 Wedde, Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats, aaO., 174

11 Vgl. Nink / Müller, Beschäftigtendaten im Konzern – Wie die Mutter so die Tochter?, in: ZD 11/2012, 508

12 Siehe hierzu ausführlich: Wedde, Beschäftigtendatenschutz und Mitbestimmungsrechte des Betriebsrats, aaO., 187; Bachner / Rupp, Die originäre Zuständigkeit des Konzernbetriebsrats bei der Einführung von technischen Einrichtungen, in: NZA 4/2016, 207 ff.

13 Schild / Tinnefeld, Datenverarbeitung im internationalen Konzern, in: DuD 9/2011, 632

ist zu dokumentieren. Ein Zuwiderhandeln ist mit Bußgeld belegt, § 43 Abs. 1 Nr. 2b BDSG.

► Vertragliche Regelung

Ein Vertrag, für dessen Abschluss der Auftraggeber verantwortlich ist, ist schriftlich abzuschließen und muss auch die Unterauftragsverhältnisse enthalten. Unterauftragsverhältnisse können zum Beispiel bei Vernichtung von Datenträgern, Fernwartung durch andere Stellen oder durch Auslagerung der Datenspeicherung gegeben sein. Ein Vertrag muss nach den Vorgaben des BDSG insbesondere folgende Inhalte haben:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Da das einzelne Unternehmen im Konzern für die Rechtmäßigkeit des Transfers an andere Unternehmen und der Verarbeitung personenbezogener Daten verantwortlich ist, wird es in einem Konzern unter Umständen einige Verträge zur Auftragsdatenverarbeitung geben müssen, wenn beispielsweise bei der Konzernmutter die IT-Abteilung oder die Personalabtei-

lung für den gesamten Konzern angesiedelt ist. Ob sich die Konzernmutter in so einem Fall von den Tochterunternehmen hinsichtlich der Verarbeitung personenbezogener Daten per Vertrag anweisen lassen will, wird in der Praxis wohl häufig sehr fraglich sein, da sie kein Interesse hat, von der Tochter kontrolliert zu werden.¹⁴

Hat die Konzernmutter eigene Befugnisse hinsichtlich des Umgangs mit den personenbezogenen Daten der Beschäftigten der Konzernunternehmen, kann keine Datenverarbeitung im Auftrag gemäß § 11 BDSG durchgeführt werden. In diesem Fall ist die Rechtmäßigkeit einer Datenübermittlung, die dann vorliegt, wie oben beschrieben gemäß § 4 in Verbindung mit § 32 BDSG zu prüfen.

Bei Datenverarbeitung im Auftrag sollte der Betriebsrat oder der GBR eine Betriebsvereinbarung abschließen, die dann über den Vertrag zur Auftragsdatenverarbeitung beim Auftragnehmer zur Wirksamkeit gebracht werden sollte. Das empfiehlt sich nachdrücklich, wenn das Unternehmen im europäischen Ausland oder im EWR seinen Sitz hat.

► Phänomen Funktionsübertragung

In Abgrenzung zur Auftragsdatenverarbeitung wird die sogenannte Funktionsübertragung diskutiert. Interessanterweise taucht dieser Begriff im Gesetz gar nicht auf¹⁵, hat aber vor einigen Jahren im Rahmen einer Novellierung Eingang in die Gesetzesbegründung zum BDSG¹⁶ gefunden und »geistert seitdem unausrottbar durch die Literatur«¹⁷.

Ein wichtiges Abgrenzungskriterium ist die Entscheidungsbefugnis über die verarbeiteten personenbezogenen Daten und die damit insgesamt verbundene datenschutzrechtliche Verantwortung. Liegt diese allein beim Auftraggeber ist der § 11 BDSG anzuwenden. Eine Funktionsübertragung und damit eine im Vorfeld nach § 4 BDSG zu prüfende Übermittlung von Personendaten soll dann vorliegen, wenn etwa dem beauftragten Unternehmen eigene Entscheidungsbefugnisse hinsichtlich des »Wie« und der Auswahl der Daten zustehen oder es die ihm übertragene Aufgabe selbstständig und weisungsfrei ausübt.

Im Grunde genommen handelt es sich dabei um eine Scheindiskussion, die das Thema Datenverarbeitung im Auftrag beziehungsweise Übermittlung personenbezogener Daten

¹⁴ Siehe Nink / Müller, Beschäftigtendaten im Konzern, aaO., 506

¹⁵ Vgl. LfDI Mecklenburg-Vorpommern, Landesdatenschutzgesetz, 43

¹⁶ BT-Drucksache 11/4306, 43

¹⁷ Ebel, Zur Abgrenzung von Auftragsdatenverarbeitung und Übermittlung, in: RDV 5/2010, 204

verkompliziert. Denn es geht hier schlicht und ergreifend um Übermitteln oder Nutzung von personenbezogenen Daten durch Dritte, deren Rechtmäßigkeit gemäß § 4 und § 32 BDSG zu prüfen ist.

Datenverarbeitung im Drittland

Sollen personenbezogene Daten in ein Drittland transferiert werden, scheidet das Privileg Datenverarbeitung im Auftrag als rechtliche Möglichkeit aus.

Denn gemäß § 3 Abs. 8 Satz 2 BDSG ist das Unternehmen im Drittland immer Dritter im Sinne des BDSG ist. Es liegt dann Übermitteln oder Nutzen personenbezogener Daten vor, was im Vorfeld in zwei Schritten zu prüfen ist. Im ersten muss Rechtmäßigkeit der Übermittlung nach § 4 in Verbindung mit § 32 BDSG gegeben und im zweiten muss nach § 4b Abs. 2 und 3 BDSG ein angemessenes Datenschutzniveau gewährleistet sein.

Wie bereits erwähnt, kann eine Übermittlung zulässig sein auf der Basis einer Einwilligung des Beschäftigten oder durch Abschluss einer Betriebsvereinbarung. Der § 32 BDSG wird nicht zum Tragen kommen, da eine entsprechende Übermittlung im Rahmen des Beschäftigungsverhältnisses im Sinne der Vorschrift nicht als erforderlich anzusehen ist. Da eine Einwilligungserklärung jederzeit widerrufen werden kann, bleibt der Abschluss einer Betriebsvereinbarung. Diese Vereinbarung muss dann in Vertragsklauseln (EU-Standardvertragsklauseln) oder verbindlichen Unternehmensregelungen in dem Unternehmen im Drittland verbindlich gemacht werden.¹⁸

Das erforderliche angemessene Datenschutzniveau für (Konzern-)Unternehmen außerhalb der EU und des EWR kann durch

- die positive Feststellung eines angemessenen Datenschutzniveaus durch die Europäische Kommission für einzelne Länder¹⁹ erfolgen
- die Vereinbarung der Geltung von EU-Standardvertragsklauseln²⁰ zur Sicherstellung eines angemessenen Datenschutzniveaus sowie

- die Einführung verbindlicher Unternehmensregelungen (Binding Corporate Rules).

Die in § 4c Abs. 1 BDSG genannten Ausnahmen für einen Datentransfer in ein Drittland ohne angemessenes Datenschutzniveau werden wohl bei Beschäftigtendaten nicht zur Anwendung kommen.

Schließen das Daten exportierende Unternehmen und der Datenimporteur einen Vertrag auf der Basis der EU-Standardvertragsklauseln ab, müssen die Verträge ohne Änderungen übernommen werden. Es empfiehlt sich jedoch, sie dahingehend zu ergänzen, dass abgeschlossene Betriebsvereinbarungen im Unternehmen im Drittland einzuhalten sind.

Die Möglichkeit des Abschlusses von verbindlichen Unternehmensregelungen bietet für den Datentransfer zwischen von Konzernunternehmen den Vorteil, dass sie an die Datenverarbeitung angepasst werden können. Es bedarf aber der Genehmigung durch die Aufsichtsbehörde.²¹

Die Sonderregelung »Safe Harbor« zwischen den USA und Europa für einen Datentransfer in die USA ist mit der Entscheidung des Europäischen Gerichtshofs vom 6.10.2015 für unzulässig erklärt worden.²² Das Nachfolgebkommen, der EU-US-Privacy-Shield, ist nicht nur in Fachkreisen höchst umstritten.²³

Fazit

Auch für betriebliche Interessenvertretungen ist der Transfer von Beschäftigtendaten innerhalb von Konzernen verbunden mit einem Transfer von Daten in Länder außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums eine Herausforderung. Der Abschluss einer Betriebsvereinbarung, die in allen Unternehmen des Konzerns über einen Vertrag zur Geltung gebracht wird, gewährleistet den Datenschutz der Beschäftigten. ◀



Bruno Schierbaum,
BTQ Niedersachsen GmbH
schierbaum@btq.de
www.btg.de

¹⁸ Vgl. Gola / Schomerus, aaO., § 4b Rn. 4

¹⁹ Positive Angemessenheitsentscheidung etwa in Bezug auf Argentinien, Uruguay, Kanada, die Schweiz, Israel und Neuseeland, in Europa kommen noch Andorra, Färöer, sowie die Inseln Guernsey, Jersey und Isle of Man hinzu; siehe hierzu Däubler / Klebe / Wedde / Weichert, BDSG, § 4b Rn. 13

²⁰ Vgl. Standardvertrag I: Entscheidung 2001/497/EG der Kommission vom 15.6.2001, Standardvertragsklauseln nach Richtlinie 95/46/EG, Abl. L 181 vom 4.7.2001, 19; Standardvertrag II: Entscheidung 2004/915/EG der Kommission vom 27.12.2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln, Abl. 385 vom 29.12.2004, 74; Standardvertrag Auftragsdatenverarbeiter: Beschluss K (2010) 593 der Kommission vom 5.2.2010, Standardvertragsklauseln nach Richtlinie 95/46/EG, Abl. L 39 vom 12.2.2010

²¹ Vgl. Nink / Müller, Beschäftigtendaten im Konzern, aaO., 507; LfD Niedersachsen, Datenübermittlung ins Ausland, 5

²² EuGH 6.10.2015 – C-362/14, siehe hierzu Weichert, Das Safe Harbor-Urteil und die Folgen, in: CuA 2/2016, 8 ff.

²³ Dazu Weichert, Das Safe-Harbor-Urteil und die Folgen, in: CuA 2/2016, 8 ff. (11); Grau / Granetzny, EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus? in: NZA 7/2016, 405 ff.