Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer

Version 1.1 | Mit Infos zu den Auswirkungen des EuGH-Urteils zu Safe Harbor und der Anwendung von Standardvertragsklauseln.

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Susanne Dehmel | Mitglied der Geschäftsleitung Vertrauen und Sicherheit
T 030 27576-223 | s.dehmel@bitkom.org

Verantwortliches Bitkom Gremium

AK Datenschutz

Satz & Layout

Sabrina Flemming | Bitkom

Titelbild

© 12521104 – istock.com

Inhaltsverzeichnis

Vorwort 4

1 Einführung: Die Übermittlung personenbezogener Daten 6

2 Rechtsrahmen 8
2.1 Anwendungsbereich des Bundesdatenschutzgesetzes 8
2.2 Spezielle Datenschutzgesetze 8
2.3 Anwendbarkeit des BDSG bei grenzüberschreitenden Sachverhalten 9
2.4 Gegenstand und Systematik des Datenschutzrechts 12

3 Datenübermittlung 14
3.1 Datenübermittlung innerhalb Deutschlands 15
3.2 Datenübermittlung in ein Land der EU/EWR 16
3.3 Datenübermittlung in ein Drittland mit angemessenem Datenschutzniveau 17
3.4 Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau 18

4 Datenübermittlung auf Grundlage ausreichender Garantien 23
4.1 Vertragsklauseln in Form individueller Datenschutzverträge 23
4.2 »Vertragsklauseln« in Form von sog. EU-Standardvertragsklauseln 23
4.3 Datenübermittlung in die USA auf Grundlage des neuen »EU-US Privacy Shields« 28
4.4 Verbindliche Unternehmensregelungen (»Binding Corporate Rules«) 29

5 Funktion einer Betriebsvereinbarung 34

6 Konzerninterne Datenübermittlung 36
6.1 Allgemeines 36
6.2 Auftragsdatenverarbeitung zwischen Konzernunternehmen 37
6.3 Zulässigkeitsnormen für die Übermittlung 37

7 Begriffsbestimmungen, Materialien, Grafiken und Übersichten 40
7.1 Begriffsbestimmungen 40
7.2 Materialien zum EU-US Privacy Shield 42
7.3 Übersicht über den weltweiten Stand des Datenschutzes 49
7.4 Entscheidungshilfe Auftragsdatenverarbeitung 52
7.5 Übersicht über die rechtlichen Mögklichkeiten der Übermittlung personenbezogener Daten in Drittländer 53
7.6 Möglichkeiten zur Erreichung eines angemessenen Datenschutzniveaus 55
7.7 §28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke 56

8 Weiterführende Links und Literatur 60

Vorwort

»Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer« war die vierte Publikation des Bitkom-Arbeitskreises Datenschutz und stammt bereits aus dem Jahr 2005. Der Arbeitskreis Datenschutz besteht aus Experten der Bitkom-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises befindet sich am Ende des Leitfadens.

Die aktualisierte Version 1.1 wurde im Sommer 2016 auf Basis des noch geltenden Rechts der EU-RL 95/46 und des Bundesdatenschutzgesetzes sowie unter Berücksichtigung der aktuellen Rechtsprechung zu Safe Harbor erstellt. Sie dient als Orientierung für die Übergangsphase bis zur endgültigen Anwendung der EU-Datenschutz-Grundverordnung ab 25. Mai 2018. Für die Zeit danach wird der Leitfaden in einer weiteren Version überarbeitet werden.

Für die Aktualisierung danken wir insbesondere folgenden Mitgliedern des Arbeitskreises:

- Arnd Böken, Graf von Westphalen Rechtsanwälte
- Jonas von Dall´Armi, Vodafone Kabel Deutschland GmbH
- Manfred Monreal, Deutsche Post AG
- Barbara Schmitz, Vodafone Kabel Deutschland GmbH

Zur ursprünglichen Version des Leitfadens hatten maßgeblich beigetragen: Anne Bernzen, Dr. Sibylle Gierschmann, LL.M., Ulrike Schroth, Regina Wacker-Dengler, Wolfgang Braun, Helmut Glaser, Alexander Heimel, Stefan Lerbs, Ralf Maruhn, Mirko Schmidt, Florian Thoma.

Die Grafiken wurden erstellt von Herrn Braun (7.7 ff), Herrn Maruhn (7.7 ff) und Herrn Thoma (7.6). Die Grafik in 7.5 und die Übersichten in 7.5 ff wurde freundlicherweise vom Autorenteam des Arbeitskreises Datenschutz und Datensicherheit der GSE Europe zur Verfügung gestellt .

Berlin, November 2016

Als weitere Publikationen des Bitkom Arbeitskreises Datenschutz sind erhältlich:

- ↗ **Mustervertragsanlage zur Auftragsdatenverarbeitung***
- Leitfaden: ↗ **Das Verfahrensverzeichnis BDSG – Ein Praxisleitfaden*** (Version 3.0). Stand März 2016.
- ↗ **FAQ – Was muss ich wissen zur EU-Datenschutz Grundverordnung?**
- ↗ **Das Safe-Harbor-Urteil des EuGH und die Folgen** Fragen und Antworten.

* *Diese beiden Leitfäden werden derzeit an die Anforderungen der Datenschutz-Grundverordnung angepasst.*

1 Einführung: Die Übermittlung personenbezogener Daten

1 Einführung: Die Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten begleitet täglich die Anbahnung und Abwicklung der Geschäfte zahlreicher Unternehmen. Ebenso wie die Geschäfte macht auch die Datenübermittlung dabei schon lange nicht mehr an den Landesgrenzen Deutschlands halt, sondern erfolgt häufig grenzübergreifend zwischen europäischen Staaten oder international. Durch die ständig zunehmende Mobilität und die Globalisierung des Welthandels gewinnt dieser grenzübergreifende Datenaustausch stetig an Bedeutung. Gefördert wird dieser Trend durch die rasante informationstechnische Entwicklung: Die weltweiten Kommunikationsmöglichkeiten über miteinander verknüpfte Netze, über die mit geringem Kostenaufwand zeitnah nahezu unbegrenzt große Datenmengen ausgetauscht werden können, hat die Datenverarbeitung endgültig von ihrer räumlichen Begrenztheit befreit. Dies betrifft nicht nur den Austausch von Daten zwischen Vertragspartnern, sondern auch den Austausch und die Weitergabe im Unternehmensverbund. In internationalen Konzernen werden z. B. häufig Personaldaten zwischen den Konzerntöchtern und der Konzernholding bzw. zwischen den Tochtergesellschaften ausgetauscht. Durch die Vernetzung der Produktions- und Handelsbeziehungen bleiben personenbezogene Daten nicht nur im Unternehmen bzw. Konzern, sondern werden auch an ausländische Geschäftspartner oder internationale Datenbanken übermittelt. So ist es bspw. erforderlich, im Rahmen von Reisebuchungen Mitarbeiterdaten an eine Vielzahl Dritter weiterzugeben. Nicht zuletzt auch im Rahmen von Outsourcing-Projekten werden Daten häufig an weltweit tätige EDV-Dienstleistungsanbieter übermittelt.

Eine grafische Übersicht über den weltweiten Stand des Datenschutzes finden Sie unter 7.3.

Nicht immer aber sind alle Beteiligten mit den rechtlichen Anforderungen einer Datenübermittlung hinreichend vertraut. Die Anforderungen sollten jedoch von jedem Unternehmen ernst genommen werden. Eine Datenübermittlung, die nicht den gesetzlichen Voraussetzungen genügt, kann als Ordnungswidrigkeit oder sogar Straftatbestand mit Bußgeldern (bis zu 300.000 Euro) bzw. Freiheitsstrafe geahndet werden (§§ 43, 44 BDSG).

Vor diesem Hintergrund will die Bitkom-Publikation »Übermittlung personenbezogener Daten« eine praktische Hilfestellung für den täglichen Gebrauch beim Transfer von Daten bieten. Neben einer kurzen Darstellung des Rechtsrahmens für die Datenübermittlung (Kapitel 2) wird vor allem die Datenübermittlung im Inland, in EU-Länder und in Drittländer erläutert (Kapitel 3 und 4). Die verschiedenen Konstellationen werden jeweils mit einem kurzen Fallbeispiel illustriert. Angesprochen wird auch die Datenübermittlung im Konzern (Kapitel 6). Abgerundet wird der Leitfaden schließlich durch ergänzende Materialien (Kapitel 7), Links und Literaturhinweise (Kapitel 8).

Bitte beachten Sie: Der Leitfaden kann angesichts der komplexen Materie keinen Anspruch auf Vollständigkeit erheben. Zudem ist die dargestellte Materie der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Letztlich versteht sich dieser Leitfaden daher als Einführung in die Problematik und Aufbereitung möglicher Handlungsmöglichkeiten, der jedoch die Einbindung professioneller unternehmensinterner oder externer Berater nicht überflüssig macht.

2 Rechtsrahmen

2 Rechtsrahmen

2.1 Anwendungsbereich des Bundesdatenschutzgesetzes

Die zentrale Rechtsgrundlage für die Übermittlung von Daten ist das Bundesdatenschutzgesetz (BDSG). Anlässlich der Umsetzung der ↗ EU-Datenschutzrichtlinie vom 24.10.1995 »zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr« (EU-RL 95/46/EG) wurde eine umfassende Novellierung des BDSG durchgeführt. Teil der Neuerungen sind die §§ 4 b und 4 c, die eigenständige Regelungen für Datenübermittlungen ins Ausland beinhalten. Die Neufassung des BDSG ist am 23.05.2001 in Kraft getretenen.

Der ↗ Text des BDSG ist (auch in englischer und französischer Sprache) abrufbar.

Das Bundesdatenschutzgesetz gilt gemäß § 1 Abs. 2 BDSG für alle öffentlichen Stellen des Bundes (Bundesverwaltung) und für die Privatwirtschaft (nicht-öffentliche Stellen), soweit sie personenbezogene Daten erheben, verarbeiten oder nutzen. Nicht-öffentliche Stellen können sein (§ 2 Abs. 4 BDSG):

- juristische Person des Privatrechts (z. B. GmbH, AG, Parteien, Vereinigungen)
- Personalgesellschaften und andere Personenvereinigungen (Gesellschaften des bürgerlichen Rechts)
- Personengesellschaften des Handelsrechts (z. B. OHG, KG)
- nicht-rechtsfähige Vereine
- natürliche Personen (gewerblich oder freiberuflich Tätige)

Die Anwendbarkeit setzt weiterhin voraus, dass die nicht-öffentliche Stelle personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, nutzt oder erhebt oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, nutzt oder dafür erhebt, ausgenommen für rein private oder familiäre Tätigkeiten (§ 1 Abs. 1 Nr. 3 BDSG).

Für die Datenverarbeitung in der Privatwirtschaft sind insbesondere die Abschnitte 1 und 3 des BDSG maßgeblich (vgl. §§ 1 Abs. 2; 27 Abs. 1 BDSG).

2.2 Spezielle Datenschutzgesetze

Das BDSG ist gemäß § 1 Abs. 3 BDSG ein Auffanggesetz. Die bereits in verschiedenen anderen Gesetzen vorhandenen spezielleren Rechtsvorschriften behalten daher ihre Gültigkeit und gehen dem BDSG vor. Dies gilt jedoch nur insoweit, als die entsprechenden Spezialgesetze eine Regelung enthalten. Fehlen solche speziellen Rechtsvorschriften dann findet für die nicht geregelten Bereiche wieder das BDSG Anwendung (Subsidiaritätsprinzip). So ist beispielsweise bei Tele-/Mediendiensten hinsichtlich der spezifischen, sich auf den jeweiligen elektronischen Kommunikationsvorgang beziehenden Daten des Nutzers das Telemediengesetz (TMG) anzuwenden. Da das TMG jedoch keine besonderen Regelungen enthält zur Erhebung, Verarbeitung und Nutzung von Inhaltsdaten, die keine Nutzungsdaten sind, bleibt für diese Bereiche das BDSG anwendbar.

2.3 Anwendbarkeit des BDSG bei grenzüberschreitenden Sachverhalten

Das BDSG geht vom »Sitzlandprinzip« aus, wonach sich das anzuwendende nationale Recht nicht nach dem Ort der Verarbeitung, sondern nach dem Sitz der verantwortlichen Stelle richtet.

Das BDSG findet aber auch auf Unternehmen, die ihren Sitz außerhalb Deutschlands haben Anwendung, wenn:

- ein Unternehmen mit Sitz in der EU oder im EWR in Deutschland eine Niederlassung hat, die die personenbezogenen Daten in Deutschland erhebt, verarbeitet oder nutzt (§ 1 Abs. 5 S. 1 BDSG).

Eine Niederlassung ist jede feste Einrichtung, von der aus eine Tätigkeit ausgeübt wird, beispielsweise von einem gemieteten Büro aus, selbst wenn die Tätigkeit nur geringfügig ist (vgl. EuGH, Urteil vom 1.10.2015, C-230/14-Weltimmo).

Beispiel: Unternehmer E mit Sitz in EU/EWR (z. B. Niederlande) betreibt eine Webseite, die auf Deutschland ausgerichtet ist, indem sie in deutscher Sprache Dienste für deutsche Kunden anbietet, und hat einen Vertreter in Deutschland, der Forderungen aus der Tätigkeit einzieht und das Unternehmen gegenüber Behörden und Gerichten vertritt (vgl. EuGH, Urteil vom 1.10.2015, C-230/14-Weltimmo).

Unternehmen E	
Sitz	
Webseite	▪ deutsche Sprache ▪ Dienste für deutsche Kunden

Vertreter	
Sitz	
Webseite	▪ zieht Forderungen ein ▪ vertritt gegenüber Behörden und Gerichten

- ein Unternehmen seinen Sitz in einem Drittland hat, aber in Deutschland Daten erhebt, verarbeitet oder nutzt, es sei denn, die Daten werden nur durchgeleitet (§ 1 Abs. 5 S. 2 BDSG).

Der Europäische Gerichtshof (EuGH) hat den Anwendungsbereich dieser Regelung erheblich ausgedehnt. Deutsches Recht gilt nicht nur für die Verarbeitung von Daten in Deutschland durch die deutsche Niederlassung. Sofern die Tätigkeiten der deutschen Niederlassung und der Muttergesellschaft außerhalb von EU/EWR untrennbar miteinander verbunden sind, gilt deutsches Recht für die gesamte Datenverarbeitung des Unternehmens (vgl. EuGH, Urteil vom 13.5.2014, C-131/12-Google Spain).

Beispiel: Unternehmen G mit Sitz in den USA betreibt eine Internetsuchmaschine, die auch in Deutschland angeboten wird. G hat eine Tochtergesellschaft in Deutschland, die Werbemöglichkeiten innerhalb der Suchmaschine anbietet.

Hier sind die Tätigkeiten der US-Muttergesellschaft und der deutschen Tochter untrennbar miteinander verbunden, da der Betrieb der Suchmaschine erst durch die Vermarktung der Werbung rentabel wird. Damit ist deutsches Recht auf die Gesamttätigkeit anwendbar, auch auf die Datenverarbeitung durch die Suchmaschine.

Muttergesellschaft G	
Sitz	
	▪ Betreibt Internetsuchmaschine

Tochtergesellschaft	
Sitz	
	▪ Vermarktet Werbemöglichkeiten in Suchmaschine

- ein Unternehmen mit Sitz in der EU oder im EWR für eine in Deutschland niedergelassene Stelle als Auftragnehmer Datenverarbeitung durchführt (§ 3 Abs. 8 S. 3 BDSG, Auftragsdatenverarbeitung, § 11 BDSG). Über § 3 Abs. 8 BDSG wird der Auftragsdatenverarbeiter in der EU oder im EWR nicht als Dritter angesehen, so dass keine Datenübermittlung vorliegt. Diese Annahme ist dann als problematisch anzusehen, wenn die Auftragsdatenverarbeitung wie etwa beim Cloud-Computing die EU/EWR-Grenzen verlässt.

Beispiel: Unternehmer A mit Sitz in Deutschland lässt die Abrechnung von Personaldaten durch ein in Norwegen ansässiges Unternehmen durchführen.

Keine Anwendung findet das BDSG, wenn eine verantwortliche Stelle mit Sitz außerhalb Deutschlands, aber innerhalb der EU/EWR, personenbezogene Daten erhebt, verarbeitet oder nutzt (§ 1 Abs. 5 S. 1 BDSG). In diesem Fall findet das am Sitz der verantwortlichen Stelle geltende Datenschutzrecht Anwendung. Ein vergleichbares Schutzniveau ist durch die jeweilige Umsetzung der EU-Richtlinie 95/46/EG sichergestellt.

Exkurs: Ausblick auf die EU DS-GVO

Am 4.5.2016 wurde die »Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Bearbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung 2016/679/EU)« im EU-Amtsblatt veröffentlicht; sie findet ab dem 25.5.2018 Anwendung. Da es sich um eine Verordnung handelt, werden die Regelungen – anders als bei der EU-Richtlinie 95/46/EG – unmittelbar gelten. Bis auf einige Ausnahmen, wie etwa im Beschäftigtendatenschutz, wird es keine spezielle nationale Gesetzgebung mehr geben.

Die DS-GVO wird zukünftig die zentrale Regelung für den privaten Bereich darstellen. Das BDSG wird nur »flankierend« wirken. Auch die Regelungen über die Datenübermittlung ins Ausland §§ 4 b und c BDSG wird es im Anwendungsbereich der DS-GVO nicht mehr geben.

Die Regelungen für die Übermittlung personenbezogener Daten an Drittländer sind in der DS-GVO im Kapitel V in den Artikeln 44 - 50 niedergeschrieben. Anwendung und Details der neuen Vorschriften werden in der nächsten Version dieses Leitfadens ausführlich dargestellt. Zum jetzigen Zeitpunkt ist hervorzuheben, dass die DS-GVO auch weiterhin für international tätige Unternehmen die gleichen Rechtsinstrumente wie z. B. die Möglichkeit der Datenübermittlung aufgrund eines Angemessenheitsbeschlusses oder aufgrund geeigneter Garantien (insbesondere Standardvertragsklauseln), bereithält. Darüber hinaus bietet die DS-GVO noch weitere Rechtsinstrumente für die internationale Übermittlung (»Codes of Conduct«, Zertifizierung).

Rechtsunsicherheiten beim Widerruf eines Angemessenheitsbeschlusses wird dadurch vorgebeugt, dass in Art. 45 Abs. 5 DS-GVO festgestellt wird, dass der Widerruf der Angemessenheit auf die Datenübermittlung keine Auswirkung hat, wenn die Datenübermittlung auf der Grundlage von geeigneten Garantien (z. B. Standardvertragsklauseln) erfolgt.

2.4 Gegenstand und Systematik des Datenschutzrechts

Als Konsequenz des Grundrechts auf »informationelle Selbstbestimmung« gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten als allgemeiner Grundsatz ein so genanntes Verbot mit Erlaubnisvorbehalt. Folglich liegt ein gesetzliches Regel-Ausnahme-Verhältnis in der Weise vor, dass die Verarbeitung fremder personenbezogener Daten regelmäßig unzulässig ist, soweit sie nicht ausnahmsweise erlaubt ist.

§ 4 Abs. 1 BDSG greift das Verbot mit Erlaubnisvorbehalt auf und erklärt eine Datenerhebung, -verarbeitung und -nutzung nur für zulässig, wenn sie durch das BDSG oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist oder der Betroffene dazu seine Einwilligung erklärt.

2.4.1 Erlaubnistatbestände

Rechtsvorschriften, die den Umgang mit personenbezogenen Daten erlauben, finden sich im BDSG in den §§ 15 Abs. 1, 16 Abs. 1, 28-32, wobei – wie im weiteren Verlauf dargestellt – § 28 BDSG von zentraler praktischer Bedeutung für den nicht öffentlichen Bereich ist.

Weitere Rechtsvorschriften, die eine Datenerhebung, -verarbeitung und -nutzung für zulässig erklären bzw. anordnen, können sich beispielsweise in bundesgesetzlichen Regelungen (Passrecht, Steuerrecht, Handelsgesetzbuch, ...), im Landesrecht und kommunalen Recht oder sonstigen bereichsspezifischen Regelungen finden, aber auch in den normativen Teilen von Tarifverträgen, Betriebsvereinbarungen, Dienstvereinbarungen etc. Auch EU-Verordnungen (z. B. Anti-TerrorVO, Verordnung EG Nr. 881/2002) können als Rechtsvorschriften, die den Umgang mit personenbezogenen Daten erlauben, in Betracht kommen, da sie für Deutschland (und jeden anderen EU-Mitgliedstaat) unmittelbare Geltung haben. Ausländische Rechtsvorschriften bleiben regelmäßig jedoch außer Betracht.

2.4.2 Einwilligung gem. § 4 a BDSG

Soll eine Einwilligung Grundlage für eine Erhebung, Verarbeitung oder Nutzung sein, ist zu beachten, dass

- die Einwilligung gemäß § 4 a Abs. 1 S. 3 BDSG der Schriftform bedarf, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist,
- der Betroffene zuvor über den konkreten Verwendungszweck zu informieren und auf vorgesehene Datenübermittlungen hinzuweisen ist (gem. § 4 a Abs. 1 S. 2 BDSG) und
- die Einwilligung auf der freien Entscheidung des Betroffenen beruhen muss, d.h. sie muss frei von Zwang sein (§ 4a Abs. 1 S. 1 BDSG).

Wenn eine Rechtsvorschrift den Umgang mit personenbezogenen Daten ausdrücklich erlaubt oder sogar anordnet, kommt es auf die Einwilligung des Betroffenen nicht an (zur Einwilligung vgl. auch noch unter Punkt 3.4.2).

3 Datenübermittlung

3 Datenübermittlung

Der Begriff der Datenübermittlung ist in § 3 Abs. 4 Nr. 3 BDSG definiert. Es handelt sich um die Phase der Datenverarbeitung, in der die geschützten personenbezogenen Daten von der verantwortlichen Stelle an andere Personen oder Stellen (Dritte) bekannt gegeben werden. Die Bekanntgabe kann durch aktive Weitergabe, gleich in welcher Form, oder durch Einsicht des Dritten oder Abruf der Daten durch einen Dritten erfolgen. Auch der Abgleich von geschützten Daten stellt eine Bekanntgabe dar. Die Weitergabe innerhalb der verantwortlichen Stelle wird hingegen nicht von dem Begriff der Übermittlung erfasst.

Eine Datenübermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG liegt nicht vor, wenn die personenbezogenen Daten im Auftrag der verantwortlichen Stelle durch einen Auftragnehmer erhoben, verarbeitet oder genutzt werden (sog. Auftragsdatenverarbeitung) und dies in der EU oder dem EWR erfolgt.

Diese Art der Privilegierung greift allerdings nur dann, wenn es sich um eine zulässige und wirksame Auftragsdatenverarbeitung im Sinne des § 11 BDSG handelt.[1] Zu beachten ist die Abgrenzung zur Funktionsübertragung. Bei einer Funktionsübertragung ist der Dienstleister nicht weisungsgebundener Auftragnehmer im Sinne von § 11 BDSG, sondern er handelt zur Wahrnehmung der an ihn übertragenen Funktion(en) bei der Datenverarbeitung mit eigenem Ermessens- und Entscheidungsspielraum, was ihn zur verantwortliche Stelle werden lässt. In diesem Fall ist dann von einer Datenübermittlung an den Dienstleister auszugehen.[2]

Abgrenzungskriterien zwischen Auftragsdatenverarbeitung und Funktionsübertragung:

Wesentliche Merkmale für eine Auftragsdatenverarbeitung sind die Weisungsabhängigkeit des Auftragnehmers gegenüber dem Auftraggeber, die fehlende vertragliche Beziehung zwischen Auftragnehmer und den Betroffenen sowie kein eigener Geschäftszweck des Auftragnehmers. Klassische Geschäftsfelder der Auftragsdatenverarbeitung sind u.a. das Cloud-Computing, Call-Center-Dienste, der Einsatz von Scan-Dienstleistern sowie die Datenträgerentsorgung und Aktenvernichtung.

Schließlich wird auch die unbefugte Weitergabe durch einen Mitarbeiter oder die Weitergabe ohne Weisung des Auftraggebers bei Bestehen eines Auftragsdatenverarbeitungsverhältnisses nicht von dem Begriff der Übermittlung erfasst.

Information

Eine Entscheidungshilfe zur Datenübermittlung im Inland, in der EU oder in Drittländer finden Sie unter Punkt 7.4!

1 Vgl. zur Frage der Privilegierung auch Schmitz/v. Dall'Armi, ZD 2016, 427ff.

2 Eine gute Gegenüberstellung der Anforderungen an die Auftragsdatenverarbeitung und die Funktionsübertragung finden Sie im ↗ **Praxisleitfaden** für Auftraggeber und Auftragnehmer des Bitkom. Dieses Dokument wird derzeit an die Anforderungen der DS-GVO angepasst.

3.1 Datenübermittlung innerhalb Deutschlands

3.1.1 Gesetzliche Erlaubnis

Wie oben bereits ausgeführt, ist § 28 BDSG die zentrale Erlaubnisnorm für die Datenübermittlung in der täglichen Unternehmenspraxis innerhalb Deutschlands. Gemäß der Vorgaben der Alternativen des § 28 BDSG ist eine Datenverarbeitung und -nutzung im nicht-öffentlichen Bereich zulässig

- bei einem Vertragsverhältnis (oder vertragsähnlichen Vertrauensverhältnis) mit dem Betroffenen, wenn es dem Zweck des Verhältnisses dient (§ 28 Abs. 1 Nr. 1 BDSG),
- wenn die Datenerhebung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung das Interesse der verantwortlichen Stelle an der Datenerhebung überwiegen (§ 28 Abs. 1 Nr. 2 BDSG),
- wenn Daten allgemein zugänglich sind oder veröffentlicht werden dürften, es sei denn, schutzwürdige Interessen des Betroffenen würden gegenüber den berechtigten Interessen der verantwortlichen Stelle offensichtlich überwiegen (§ 28 Abs. 1 Nr. 3 BDSG).

sowie u. a. auch

- bei der Übermittlung von Stammdaten zu Marketingzwecken (Werbung, Markt- und Meinungsforschung bei listenmäßig oder sonst zusammengefassten Daten über Angehörige einer Personengruppe, § 28 Abs. 3 BDSG).

Besteht ein Vertragsverhältnis zwischen der verantwortlichen Stelle und dem Betroffenen, so ist, um die Schutzwirkung nicht zu unterlaufen, vorrangig § 28 Abs.1 Nr. 1 BDSG anzuwenden. Für die Berufung auf »berechtigte Interessen« der verarbeitenden Stelle nach § 28 Abs. 1 Nr. 2 BDSG bleibt deshalb bei Bestand einer vertraglichen Beziehung, wie z. B. einem Arbeitsverhältnis, einem Bankvertrag oder einem auf einem besonderen Vertrauensverhältnis basierenden Vertragsverhältnis, nur ein eingeschränkter Anwendungsbereich zu § 28 BDSG vgl. auch unter Punkt 7.7.

Information

Eine ausführliche grafische Darstellung der Erlaubnistatbestände des § 28 BDSG finden Sie unter Punkt 7.7!

3.1.2 Einwilligung des Betroffenen

- Eine Datenübermittlung ist auch möglich, wenn der Betroffene eingewilligt hat. Zusätzlich zum Vorliegen der gesetzlichen Voraussetzungen einer Einwilligung (vgl. Punkt 2.4.2) sind dabei jedoch mehrere Punkte zu beachten, die sich in der Praxis als problematisch erweisen können:

- Der Kreis der Betroffenen sollte überschaubar sein (Unternehmensgröße).

- Die verantwortliche Stelle muss die Betroffenen über jeden beabsichtigten Verarbeitungszweck konkret informieren, u. U. ist daher (bei geändertem oder erweitertem Verarbeitungszweck) auch eine Aktualisierung erforderlich.
- Es muss die Möglichkeit in Betracht gezogen werden, dass einzelne Betroffene die Einwilligung nicht erteilen oder später widerrufen, was die gesamte Maßnahme in Frage stellen kann.
- Bei Arbeitnehmerdaten: Nach wie vor umstritten ist die Frage, ob im Arbeitsverhältnis überhaupt wirksam eingewilligt werden kann, da der theoretischen Entscheidungsfreiheit des Arbeitnehmers ein faktisches Abhängigkeitsverhältnis gegenüber stehen kann. Hier ist gem. § 94 BetrVG u. U. auch die Zustimmung des Betriebsrates für Einwilligungserklärungen in Personalfragebögen oder Formulararbeitsverträgen einzuholen. Tatsächlich dürfte die Datenerhebung bei Arbeits- und Dienstverhältnissen im Regelfall mit Bezug zur konkreten Tätigkeit häufig im Rahmen des § 28 Abs. 1 Nr. 1 BDSG erfolgen.

In der Praxis ist die Einwilligung daher häufig nur eine bedingt geeignete Lösung.

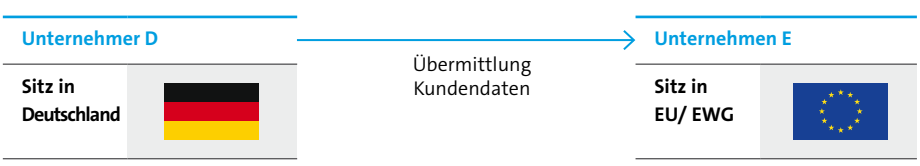
3.2 Datenübermittlung in ein Land der EU/EWR

Durch die Umsetzung der EU-Datenschutzrichtlinie 95/46/EG in allen Mitgliedstaaten der EU wurde ein weitgehend einheitliches und adäquates Schutzniveau für personenbezogene Daten eingeführt (»Angemessenes Datenschutzniveau«). Auch für die EWR-Staaten Norwegen, Island, Liechtenstein ist die Angemessenheit des Datenschutzniveaus anerkannt. Diese Länder sind bezüglich der Datenübermittlung daher mit Ländern innerhalb der EU gleichzusetzen.

Das hat zur Folge, dass der Datenverkehr innerhalb der Mitgliedstaaten der Europäischen Union und mit den EWR-Staaten im Anwendungsbereich des Gemeinschaftsrechts genauso zu behandeln ist wie die inländische Datenübermittlung (vgl. § 4 b Abs. 1 BDSG) und in diesem Rahmen zulässig ist.

Für den Fall, dass ein deutsches Unternehmen Daten in ein anderes EU/EWR-Land übermitteln will, kann daher in vollem Umfang auf die Ausführungen in Punkt 3.1 verwiesen werden.

Beispiel: Unternehmer D mit Sitz in Deutschland übermittelt Kundendaten an das Unternehmen E mit Sitz in der EU/EWG (z. B. Spanien).



3.3 Datenübermittlung in ein Drittland mit angemessenem Datenschutzniveau, § 4 b Abs. 2 BDSG

Das BDSG geht davon aus, dass die Übermittlung von Daten an ausländische Stellen außerhalb der EU/EWR unterbleiben muss, wenn der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Ein solches entgegenstehendes schutzwürdiges Interesse ist insbesondere dann anzunehmen, wenn bei der empfangenden Stelle die Angemessenheit des Datenschutzniveaus nicht gegeben ist, § 4 b Abs. 2 S. 2 BDSG.

- Hieraus ergibt sich zunächst, dass eine Datenübermittlung in ein Drittland rechtmäßig möglich ist, wenn die Angemessenheit des Niveaus der Datenschutzgesetzgebung dieses Landes anerkannt ist und keine anderen schutzwürdigen Interessen des Betroffenen entgegenstehen.

- Ist das Datenschutzniveau eines Landes nicht durch einheitliche Gesetze gesichert, kann eine Angemessenheit im Sinne des § 4 b Abs. 2 BDSG gleichwohl dann angenommen werden, wenn eine Vereinbarung des Landes mit der EU getroffen wurde, die ein angemessenes Datenschutzniveau sicherstellt und der Übermittlungsempfänger dieser Vereinbarung beigetreten ist (Beispiel: Privacy Shield der EU und den USA, dazu unter 4.3.).

Hat ein Drittland ein angemessenes Datenschutzniveau, ist eine Datenübermittlung rechtmäßig möglich, wenn nicht sonstige schutzwürdige Interessen des Betroffenen dem entgegenstehen. Die Feststellung der Angemessenheit erfolgt in einem förmlichen Verfahren durch die EU-Kommission (Art. 25 Abs. 6 EU-Datenschutzrichtlinie).

Ein angemessenes Datenschutzniveau wurde von der EU-Kommission in einer förmlichen Entscheidung für folgende Länder festgestellt:

- Argentinien (2003/490/EC)
- Andorra (2010/625/EU)
- Guernsey (2003/821/EC)
- Isle of Man (2004/411/EC)
- Jersey (2008/393/EC)
- Kanada (2002/2/EC)
- Neuseeland (2013/65/EU)
- Israel (2011/61/EU)
- Schweiz (2000/518/EC)
- Färöer Inseln (2010/146/EU)
- Uruguay (2012/484/EU)

Die Angemessenheit des Datenschutzniveaus bedeutet dabei nicht zwingend, dass die Verhältnisse gleichartig oder gleichwertig sind.

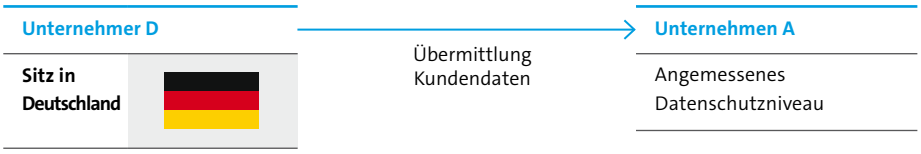
Information

Eine tabellarische Darstellung der Möglichkeiten der Übermittlung in Drittländer finden Sie unter Punkt 7.5!

Zurzeit wird von der Kommission dem Vernehmen nachgeprüft, ob die Länder Japan, und Australien ein angemessenes Datenschutzniveau aufweisen, die Entscheidungen stehen jedoch noch aus.

Weitere Informationen zu den Entscheidungen der Kommission können auf der ↗EU-Datenschutz-Homepage abgerufen werden.

Beispiel: Unternehmer D mit Sitz in Deutschland übermittelt z. B. Kundendaten an das Unternehmen A mit einem angemessenen Datenschutzniveau (z. B. Schweiz, Guernsey, Argentinien, Kanada, etc.).



3.4 Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau

Auch in Fällen, in denen für das betreffende Drittland kein angemessenes Datenschutzniveau festgestellt wurde, kann eine Datenübermittlung möglich sein. Der Grundsatz des § 4b Abs. 2 S.2 BDSG wird duch mehrere Ausnahmen durchbrochen:

- § 4 c Abs. 1 Nr. 1 und Nr. 2 BDSG ermöglichen als Ausnahmevorschriften Übermittlungen an Stellen ohne angemessenes Datenschutzniveau, wenn der Betroffene eingewilligt hat oder die Übermittlung zur Erfüllung eines Vertrags mit dem Betroffenen notwendig ist (siehe dazu unter 3.4.1 und 3.4.2).

- Eine Datenübermittlung nach § 4 c Abs. 2 BDSG schließlich setzt voraus, dass das fehlende angemessene Datenschutzniveau durch ausreichende Garantien ausgeglichen wird. Die Garantien können sich insb. aus Vertragsklauseln (dazu unter 4.1 und 4.2) und verbindlichen Unternehmensregelungen ergeben (dazu und zum Streit um die Einordnung von Unternehmensregelungen unter Punkt 4.4).

Diese Übermittlungsmöglichkeiten und ihre Voraussetzungen werden in den folgenden Abschnitten erläutert.

Information

Eine grafische Darstellung der §§ 4b und 4c BDSG finden Sie unter Punkt 7.6!

Hinweis

Die Voraussetzungen für eine rechtmäßige Übermittlung im Inland (z. B. nach § 28 BDSG) sind auch bei einer Datenübermittlung in ein Drittland relevant, denn bei jeder Datenübermittlung ins Ausland muss neben der Frage nach den speziellen Voraussetzungen für die Übermittlung in ein bestimmtes Land (§§ 4 b und 4 c BDSG) zusätzlich geprüft werden, ob darüber hinaus auch die allgemeinen Voraussetzungen für eine Übermittlung vorliegen (§ 4 Abs. 1, 28 BDSG, zu § 28 BDSG vgl. oben X). Erforderlich ist also eine ZWEISTUFIGE PRÜFUNG.

3.4.1 Ausnahme 1: Zur Vertragserfüllung notwendige Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau

Eine Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau ist ausnahmsweise zulässig, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein Vertrag abgeschlossen worden ist, für dessen Erfüllung die Datenübermittlung erforderlich ist, § 4 c Abs. 1 Nr. 2 BDSG. In gleicher Weise ist eine Datenübermittlung zulässig, die zur Durchführung von vorvertraglichen Maßnahmen erforderlich ist.

Der praktische Anwendungsbereich dieser Zulässigkeitsalternative liegt neben dem internationalen Zahlungsverkehr und Kaufverträgen im Fernabsatz vor allem im Tourismusgewerbe. Die Durchführung von vertraglichen Vereinbarungen über internationale Beförderungsleistungen, Reservierungen von Mietwagen, Unterkünften oder Hotelzimmern in Drittländern wird so ermöglicht.

Beispiel: Kunde K möchte, dass sein Reisebüro für ihn in Sydney ein Hotelzimmer reserviert. Das Reisebüro kann sich für die Übermittlung der Daten des K an das Hotel in Sydney auf § 4 c Abs. 1 Nr. 1 BDSG berufen, da zur Durchführung bzw. Erfüllung des Vertrages zwischen Kunde K und dem Reisebüro die Weitergabe seiner Daten zwingend notwendig ist.

Ein Vertrag i.S.d. Nr. 2 kann auch ein Arbeitsvertrag sein, so dass die Übermittlung von Arbeitnehmerdaten in ein Drittland auf Grund eines Arbeitsvertrages zulässig sein kann. Entscheidend für die Beurteilung der Zulässigkeit ist, ob die Übermittlung für die Durchführung bzw. Erfüllung der jeweiligen einzelnen Regelung des Arbeitsvertrags erforderlich ist. Dies ist für jeden Arbeitnehmer gesondert zu prüfen. Denkbar ist die Zulässigkeit der Datenübermittlung z. B., wo der Mitarbeiter zu Auslandseinsätzen verpflichtet ist oder bei der Gewährung von Aktienbezugsrechten, die in einem Drittland verwaltet werden.

Etwas anders liegt die Konstellation, für die § 4 c Abs. 1 Nr. 3 BDSG die Zulässigkeit einer Datenübermittlung begründen kann. Nach der Nr. 3 kann eine Übermittlungen zulässig sein, die zur Erfüllung eines Vertrags notwendig ist, der zwar nicht vom Betroffen selbst mit der verantwortlichen Stelle geschlossen wurde, aber im Interesse des Betroffenen zwischen der verantwortlichen Stelle und einem Dritten.

Beispiel: Der Arbeitgeber überträgt Daten eines Arbeitnehmers, für den er eine Mitarbeiterversicherung abgeschlossen hat, an eine ausländische Versicherungsgesellschaft. Häufig wird es sich bei der Anwendung der Nr. 3 um Verträge zugunsten Dritter i.S.d. § 328 BGB handeln.

Zu beachten ist bei allen Zulässigkeitsalternativen des § 4 c Abs. 1, dass der Datenempfänger darauf hinzuweisen ist, dass die Daten nur zweckgebunden verarbeitet oder genutzt werden dürfen (vgl. § 4 c Abs. 1 S. 2 BDSG), wobei sich der Zweck z. B. aus dem Vertrag ergibt.

3.4.2 Ausnahme 2: Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auf der Grundlage einer Einwilligung

Wie bei der Datenübermittlung innerhalb Deutschlands oder innerhalb der EU/EWR kann auch eine Datenübermittlung in ein Drittland auf der Grundlage einer Einwilligung des Betroffenen zulässig sein, § 4 c Abs. 1 Nr. 1 BDSG.

Für die Einwilligung in die Drittlandübermittlung von Daten gelten die schon in Punkt 2.4.2 dargestellten, strengen Anforderungen, ebenso wie die in Punkt 3.1.2 erläuterten praktischen Schwierigkeiten.

Beim Datentransfer in ein Drittland kann jedoch noch eine weitere Schwierigkeit hinzutreten, denn nach überwiegender Ansicht ist der Betroffene (zusätzlich zu den oben aufgeführten Umständen der Datenübermittlung) umfassend über die Risiken der Übermittlung seiner Daten in ein Land ohne ausreichendes Datenschutzniveau zu informieren (vgl. § 4 a BDSG). Erforderlich ist also die Transparenz bezüglich der Schutzmaßnahmen bzw. Datenschutzgarantien bei der empfangenden Stelle oder im Empfängerland.

Die in Punkt 3.4.1 erwähnte Zweckbindung mit Hinweispflicht gilt auch hier.

3.4.3 Ausnahme 3: Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auf Grundlage ausreichender Garantien

Neben den vorgenannten Möglichkeiten kann die Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auch auf Grundlage »ausreichender Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte« erfolgen (vgl. § 4c Abs. 2 BDSG). Anders als bei Feststellungen über die Angemessenheit des Datenschutzniveaus nach Art. 25 Abs. 6 der EU Datenschutzrichtlinie kommt es hier nicht auf das Datenschutzniveau im betreffenden Drittland, sondern auf die (vertraglichen) Zusicherungen der kontrahierenden Stellen in Hinblick auf den Schutz der Persönlichkeitsrechte der Betroffenen an. Dazu kann der Datenexporteur entweder eigene »Vertragsklauseln« oder verbindliche Unternehmensregelungen (sogenannte Binding Corporate Rules) mit ausreichenden Garantien entwickeln oder auf die von der Kommission verabschiedeten »Standardvertragsklauseln« zurückgreifen.

Diese Instrumente werden in Kapitel 4 ausführlich erläutert.

3.4.4 Datenübermittlung in ein Drittland auf Anweisung einer Behörde

Auch bei der Datenübermittlung in ein Drittland auf Anweisung einer Behörde gilt, dass eine Datenübermittlung in ein Drittland nur zulässig ist, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist (§ 4 b Abs. 2 BDSG) und wenn die Datenübermittlung auf Grundlage eines Gesetzes oder einer Rechtsvorschrift erfolgt (§ 4 Abs. 1 BDSG).

Als Beispiel für eine Datenübermittlung in ein Drittland kann hier das Abkommen zur Flugdatenweitergabe mit den USA auf Basis der EU-Regelungen verwendet werden. Dieses Abkommen verpflichtet die Fluggesellschaften einen Teil der Flugdaten aller Passagiere, die in die USA reisen, den amerikanischen Behörden zum Abruf zur Verfügung zu stellen. Ähnliche Abkommen gibt es derzeit mit Australien und Kanada.

Ein Verfahren, bei dem die Daten zur Verfügung gestellt werden und vom Empfänger abgerufen werden können, ist nach § 3 Abs. 4 Nr. 3 BDSG als Datenübermittlung einzustufen.

Die EU-Kommission hat mit ihrer Entscheidung vom 14. Mai 2004 die Angemessenheit des Schutzniveaus für die Verarbeitung von Flugpassagierdaten in den Vereinigten Staaten anerkannt. Mit Bestätigung des Schutzniveaus wurde am 17. Mai 2004 das Abkommen zur Übermittlung der Flugpassagierdaten beschlossen, das mittlerweile mehrmals angepasst wurde. Das neueste Abkommen ist vom 11. August 2012. Damit ist für die Fluggesellschaften zunächst die erforderliche Rechtsgrundlage (§ 4 Abs. 1 BDSG) gegeben, ein angemessenes Datenschutzniveau liegt vor (§ 4 b Abs. 2 BDSG) und die Datenübermittlung ist daher rechtmäßig.

Abkommen zwischen den Vereinigten Staaten von Amerika und der Europäischen Union über die Verwendung von Fluggastdatensätzen und deren Übermittlung an das United States Department of Homeland Security (2012):
↗ http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:22012A0811(01)&from=EN

Mehr Infos zu Fluggastdatenabkommen der EU: ↗ http://ec.europa.eu/justice/data-protection/international-transfers/pnr-tftp/pnr-and-tftp_en.htm

4 Datenübermittlung auf Grundlage ausreichender Garantien

4 Datenübermittlung auf Grundlage ausreichender Garantien

4.1 »Vertragsklauseln« in Form individueller Datenschutzverträge

Zwischen dem Datenexporteur und -importeur kann ein individueller, d. h. selbst formulierter Vertrag zum Datenschutz geschlossen werden, der von der zuständigen Aufsichtsbehörde – bei Post- und Telekommunikationsunternehmen durch den/die Bundesbeauftragte(n) für den Datenschutz und die Informationsfreiheit (BfDI) – genehmigt werden muss. Prüfungsmaßstab sind die Persönlichkeitsrechte, Grundrechte und Grundfreiheiten, die in der EU-Grundrechtscharta manifestiert sind. Nur wenn zum Schutz dieser Rechte und Freiheiten sowie der Ausübung der damit verbundenen Rechte ausreichende Garantien vorhanden sind, kann eine Genehmigung erteilt werden. Für die Praxis ist zu beachten, dass ein solches Genehmigungsverfahren langwierig sein kann.

4.2 »Vertragsklauseln« in Form von sog. EU-Standardvertragsklauseln

Basierend auf Art. 26 Abs. 4 der EU Datenschutzrichtlinie hat die Kommission Standardvertragsklauseln für unterschiedliche Fallkonstellationen verabschiedet, welche an Stelle der vorgenannten individuellen Vertragsklauseln verwendet werden können:

- Standardvertragsklauseln für die Datenübermittlung zwischen für die Verarbeitung Verantwortlichen (Controller-Controller-Transfer)
  - Set I aus der Entscheidung 2001/497/EG vom 15. Juni 2001
  - Set II (sog. alternative Standardvertragsklauseln) aus der Entscheidung 2004/915/EG vom 27. Dezember 2004 zur Änderungen der Entscheidung 2001/497/EG
- Standardvertragsklauseln für die Datenübermittlung zwischen für die Verarbeitung Verantwortlichen und nach deren Weisung handelnden Auftragsverarbeitern (Controller-Prozessor-Transfer):
  - Beschluss 2010/87/EU vom 5. Februar 2010 (die früheren Standardvertragsklauseln zur Auftragsverarbeitung aus der Entscheidung 2002/16/EG vom 27. Dezember 2001 gelten nur für vor dem 15.5.2010 geschlossene Verträge)

Während für Datenübermittlungen zwischen verantwortlichen Stellen und ihren Auftrags(daten)verarbeitern lediglich ein Typ Standardvertragsklauseln existiert, besteht bei Datenübermittlungen zwischen verantwortlichen Stellen die Wahlmöglichkeit aus zwei Sets. Diese unterscheiden sich insbesondere hinsichtlich der Haftung, Bindung an aufsichtsbehördliche Hinweise bzw. Entscheidungen und die Gestaltungs- bzw. Ergänzungsspielräume. Allerdings ist das Set II

aufgrund der eingeschränkten Haftung und Auskunftspflicht des Datenexporteurs und den hieraus resultierenden Wertungswidersprüchen zum deutschen Recht grundsätzlich nicht geeignet für die Übermittlung von Beschäftigtendaten.[3] Das Set II wurde von der Internationalen Handelskammer unter Beteiligung weiterer Wirtschaftsverbände mit der Kommission ausgehandelt, um Schwächen der Standardvertragsklauseln vom Juni 2001 auszugleichen. Diese »alternativen Klauseln« werden daher von vielen Unternehmen insgesamt als vorzugswürdig eingestuft.

Set I (2001/497/EG vom 15.6.2001)	Set II (2004/915/EG vom 27.12.2004), alternative Klauseln
Gesamtschuldnerische Haftung *vgl. Klausel 6*	Jede Partei haftet für eigenes Verschulden; Strafschadenersatzansprüche (punitive damages) sind ausgeschlossen; *vgl. Ziffer III* Aber: wegen Haftungseinschränkung grundsätzlich nicht geeignet für Beschäftigtendaten
strengere Bindung an (unverbindliche) Ratschläge (»advice«) der Aufsichtsbehörden *vgl. Klausel 5*	Bindung an bestandskräftige (verbindliche) Entscheidungen (»decisions«) der Aufsichtsbehörden *vgl. Ziffer V*
Klauseländerungsverbot *vgl. Klausel 11*	Erlaubnis für ergänzende Verträge zur Regelung kommerzieller Fragen; Beschreibung der Übermittlung in Anhang B, kann angepasst und ergänzt werden *vgl. Ziffer VII*

Bei der Verwendung von Standardvertragsklauseln ist darauf zu achten, dass die vorgegebenen Klauseln von den Vertragspartnern grundsätzlich nicht verändert oder durch Nebenabreden anderweitig eingeschränkt werden dürfen. Ergänzungen sind nur im Rahmen sog. geschäftlicher Klauseln zulässig, soweit die betreffenden Standardvertragsklauseln eine solche Ergänzung zulassen und solange diese nicht direkt oder indirekt im Widerspruch zu den Standardvertragsklauseln stehen oder Grundrechte oder Grundfreiheiten der betroffenen Personen verletzen. Im Fall einer unzulässigen Änderung verlieren die Klauseln ihren privilegierten Status als Standardvertragsklauseln im Sinne des Art. 26 Abs. 4 der EU Datenschutzrichtlinie und unterliegen sodann als »einfache« Vertragsklauseln der Genehmigungspflicht. Erfolgt die Übermittlung hingegen auf Basis von (unveränderten) Standardvertragsklauseln bedarf es nach deutschem Datenschutzrecht hingegen keiner Genehmigung durch die Aufsichtsbehörde, da die Kommission im Rahmen des Verfahrens nach Art. 26 Abs. 4 i.V.m. Art. 31 Abs. 2 der EU Datenschutzrichtlinie ja bereits die Feststellung getroffen hat, dass die Standardvertragsklauseln ausreichende Garantien zum Schutz der Persönlichkeitsrechte der Betroffenen enthalten. Allerdings können Aufsichtsbehörden die Vorlage der vereinbarten Standardvertragsklauseln verlangen.[4]

Hinweis

In anderen EU-Staaten (z. B. AT, HR, CY, EE, FR, IS, LV, LT, LU, MT, RO, SI, ES) kann eine Genehmigung auch im Fall von Standardvertragsklauseln erforderlich sein. Im Zweifelsfall sollten sich Unternehmen bei ihrer zuständigen Aufsichtsbehörde informieren.

3 Vgl. Abgestimmte Positionen der Aufsichtsbehörden in der AG »Internationaler Datenverkehr« am 12./13. Februar 2007, Seite 2, II.2.

4 Weiterführend zum Thema Standardvertragklauseln Schmitz/v. Dall'Armi, ZD 2016, 217ff.

Exkurs: Anwendbarkeit der Standardvertragsklauseln nach dem EuGH-Urteil zu Safe Harbor vom 6.10.2015

Mit der Angemessenheitsentscheidung »Safe Harbor« hatte die EU-Kommission die Voraussetzung geschaffen, ein angemessenes Datenschutzniveau im Sinne von Art. 25. Abs. 2 DS-RL für den Transfer personenbezogener Daten in die USA anzunehmen, wenn sich der Importeur in den USA den Safe-Harbor-Prinzipien und den sog. »Frequently Asked Questions« unterwirft. Diese Entscheidung hat der EuGH mit seiner Entscheidung vom 6. Oktober 2015 (sog. »Schrems-Urteil«) jedoch für unwirksam erklärt. Mit der Folge, dass der Datentransfer in die USA auf der Grundlage der Safe Harbor-Feststellung spätestens seit Ende Januar 2016 nicht mehr zulässig ist (siehe dazu ↗ Positionspapier der Datenschutzkonferenz und ↗ der Art. 29 Datenschutzgruppe).

Neben der Möglichkeit der Datenübermittlung auf der Grundlage einer Angemessenheitsfeststellung besteht die Möglichkeit einer Datenübermittlung in Länder ohne angemessenes Datenschutzniveau auf der Grundlage von Standardvertragsklauseln. Art. 26 Abs. 4 DS-RL ermächtigt die Kommission, solche Vertragsklauseln in einem Verfahren nach Art. 31 Abs. 2 DS-RL zu erarbeiten und als sog. Standardvertragsklauseln festzuschreiben.

Die Standardvertragsklauseln dienen dem Zweck, die Übermittlung personenbezogener Daten zwischen dem Datenexporteur und dem Datenimporteur unabhängig vom Datenschutzniveau des Drittlands zu legitimieren.

Nach überwiegender Auffassung der Aufsichtsbehörden, der Literatur und der EU-Kommission haben die Standardvertragsklauseln mit dem EuGH-Urteil nicht ihre Gültigkeit verloren und können daher bis auf weiteres weiterverwendet werden. Insbesondere obliegt die Befugnis, eine Entscheidung der Kommission über Standardvertragsklauseln für unwirksam zu erklären, allein dem EuGH (Vgl. Urteil des Europäischen Gerichtshof Az.: C-362/14, sog. Safe-Harbor oder Schrems-Urteil, RZ 61). Solange eine solche Feststellung nicht vorliegt, ist die Entscheidung der Kommission nach Art. 288 Abs. 4 AEV für alle Organe der Mitgliedstaaten verbindlich (Vgl. Urteil des Europäischen Gerichtshof Az.: C362/14, sog. Safe-Harbor oder Schrems-Urteil, RZ 51).

Davon unberührt bleibt die Möglichkeit der Aufsichtsbehörden, Datenübermittlungen im Rahmen ihrer Zuständigkeit und Kraft ihrer Befugnisse zu unterbinden bzw. zu sanktionieren. Eine zentrale Befugnis hierzu ergibt sich aus den Entscheidungen der Kommission über die jeweiligen Standardvertragsklauseln, wonach die Kontrollstelle die Datenübermittlung unter anderem verbieten oder aussetzen kann, wenn einzelne Klauseln der Standardvertragsklauseln von den Vertragsparteien nicht eingehalten werden.

Insoweit wird es entscheidend darauf ankommen, wie die Standardvertragsklauseln umgesetzt und in der Praxis gelebt werden. Die Frage, ob Aufsichtsbehörden darüber hinaus auch Entscheidungen darüber treffen können, ob Rechtsvorschriften im Drittland den Datenimporteur zwingen, »[...] von den einschlägigen Datenschutzvorschriften in einem Maß abzuweichen, das über die Beschränkungen hinausgeht, die im Sinne von Art. 13 der Richtlinie 95/46/EG für eine demokratische Gesellschaft erforderlich sind« und sich dies »[...]wahrscheinlich sehr nachteilig auf die Garantien auswirk[t], die die Standardvertragsklauseln bieten sollen« (siehe Art. 4 Abs. 1 lit. a der Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001) , ist nicht eindeutig zu beantworten. Mit Blick auf (1) die Formulierung der aufsichtsbehördlichen Rechte in den jeweiligen Kommissionentscheidungen, (2) den Prüfungsmaßstab, den es bei der Beurteilung der vorgenannten Fragen zu beachten gilt und (3) das den Kontrollstellen nach Art. 28 Abs. 3 der RL 95/46/EG zustehende Klagerecht, auf das der EuGH in seiner Entscheidung zu Safe Harbor ausdrücklich hinweist, spricht vieles dafür, eine diesbezügliche Entscheidungsbefugnis unter Berücksichtigung auch der Harmonisierungsgedanken der Kommission bzw. dem EuGH zuzusprechen (Vgl. Schmitz/von Dall´Armi, ZD 2016, 217). Der weitere Verlauf der Diskussion, insbesondere die Positionierung der Artikel-29-Datenschutzgruppe sowie einzelner Aufsichtsbehörden zum Thema Standardvertragsklauseln ist weiterhin zu beobachten.

Die Standardvertragsklauseln sowie weitere Informationen sind unter den folgenden Links eingestellt:

- ↗ Set I aus der Entscheidung 2001/497/EG vom 15. Juni 2001 (Controller-Controller-Transfer)
- ↗ Set II (sog. alternative Standardvertragsklauseln) aus der Entscheidung 2004/915/EG vom 27. Dezember 2004 zur Änderungen der Entscheidung 2001/497/EG (Controller-Controller-Transfer)
- ↗ Standardvertragsklauseln für Auftragsverarbeiter (Controller-Prozessor-Transfer)
- ↗ EU-Kommission
- ↗ Internationale Handelskammer

Exkurs: Nicht mehr zulässige Datenübermittlung in die USA auf Grundlage der »Safe Harbor Principles«

~~Safe Harbor~~

Da in den USA kein einheitlich normiertes Datenschutzrecht existiert, das dem Betroffenen »ausreichende Garantien« im Sinne des europäischen Datenschutzes zur Verfügung stellt, bedarf eine Übermittlung von personenbezogenen Daten in die USA der Absicherung durch die beteiligten Unternehmen. Zu diesem Zweck haben sich im Jahr 2000 die EU-Kommission und die amerikanische Regierung auf das sog. Safe Harbor Paket geeinigt. Das Safe-Harbor-Paket bestand aus sieben Datenschutzprinzipien und 15 sog. »Frequently Asked Questions, FAQ«. Unterwarf sich ein amerikanisches Unternehmen den Prinzipien, konnte das deutsche, übermittelnde Unternehmen von einem »angemessenen Datenschutzniveau« ausgehen.

Die Entscheidung 2000/520 der EU-Kommission aus dem Jahr 2000, mit der das durch Safe Harbor hergestellte Datenschutzniveau als angemessen anerkannt wurde, wurde jedoch vom Europäischen Gerichtshof am 6.10.2015 für ungültig erklärt.

Eine zukünftige Datenübermittlung auf Basis dieser Rechtsgrundlage ist damit nicht mehr zulässig. Unternehmen, die nicht auf andere Rechtsgrundlagen (wie Standardvertragsklauseln) umstellen, droht ein Bußgeld. In Deutschland wurden bereits erste Bußgelder von Datenschutzaufsichtsbehörden (Hamburg) verhängt.

Im Juli 2016 haben die EU und USA ein neues Abkommen verabschiedete, das sogenannte »EU-US Privacy Shield«. Amerikanische Unternehmen können sich, ähnlich wie schon zuvor bei Safe Harbor, in eine entsprechende Liste eintragen lassen und sich selbst dazu verpflichten, die in dem Datenschutzschild gemachten datenschutzrechtlichen Vorgaben einzuhalten (mehr Informationen unter Punkt 4.3).

Weitere Informationen zu dem Safe Harbor Urteil des EuGH finden Sie in den ↗ FAQ, die der Bitkom kurz nach der Entscheidung bereitgestellt hat.

Weitere Informationen zur Ungültigkeit von Safe Harbor:

- ↗ Mitteilung zu der Übermittlung personenbezogener Daten aus der EU in die USA nach dem Urteil des Gerichtshofs in der Rechtssache C-362/14 (Schrems)
- ↗ Information der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

4.3 Datenübermittlung in die USA auf Grundlage des neuen »EU-US Privacy Shields«

Privacy Shield

Die EU-Kommission hat am 12. Juli 2016 den »EU-US Datenschutzschild« (eng. »Privacy Shield«) angenommen. Das Privacy Shield ist eine »Angemessenheitsentscheidung« (C (2016) 4176 final) der EU-Kommission gem. Art. 25 Abs. 6 der Datenschutzrichtlinie 95/46/EG, die durch ergänzende Dokumente (»Anhänge«) ergänzt wird. Der Umsetzungsbeschluss wurde an die EU-Mitgliedsstaaten zugeleitet und trat damit unverzüglich in Kraft.

Im Rahmen des Privacy Shields verpflichten sich US-Unternehmen die in den Dokumenten gemachten datenschutzrechtlichen Vorgaben einzuhalten. Dafür stellt ihnen das US-Handelsministerium ab 1. August 2016 eine Bescheinigung aus und trägt sie in eine entsprechende Liste auf seiner ↗ Webseite ein. Sobald US-Unternehmen zertifiziert sind, wird fingiert, dass ein angemessenes Datenschutzniveau besteht. Der Abschluss von Standardvertragsklauseln oder anderer Maßnahmen ist für den Datenaustausch mit entsprechenden zertifizierten Unternehmen nicht mehr erforderlich.

Regelungsinhalte des Privacy Shield:

- Strenge Auflagen für Unternehmen, die Daten verarbeiten
  - Info über:
    - Teilnahme am Privacy Shield
    - Arten der personenbezogenen Daten
    - Verpflichtung die Grundsätze des Privacy Shield einzuhalten
    - Zweckbestimmung der Datenerhebung/-verarbeitung
    - Kontaktangabe für Beschwerden
    - Info wenn Daten an Dritte weitergegeben werden sollen
    - Betroffenenrechte auch für EU-Bürger (Beschwerderecht/Auskunftsrecht)
  - regelmäßige Überprüfung der teilnehmenden Unternehmen bzgl. der Anforderungen
  - werden die Anforderungen nicht eingehalten, erfolgt eine Streichung von der Liste
  - strenge Auflagen gelten auch im Falle einer Datenweitergabe
- Transparenzpflichten beim Datenzugriff durch US-Behörden
- Sammelerhebung von Daten nur unter bestimmten Voraussetzungen und mit einer möglichst gezielten Ausrichtung
- Ombudsstelle, an die sich EU-Bürger mit Rechtsschutzbegehren wenden können. Dieser Rechtsschutz gilt auch für andere Instrumente wie z. B. Standardvertragsklauseln und verbessert damit den Rechtsschutz gegen Zugriffe auf Behörden insgesamt.

- Gemeinsame jährliche Überprüfung durch US-Handelsministerium und EU-Kommission: Überprüft wird die Funktionsweise des Datenschutzschilds einschließlich der Zusicherungen und Zusagen hinsichtlich des Datenzugriffs aus Gründen der Rechtsdurchsetzung oder der nationalen Sicherheit.

Weitere Informationen hierzu finden Sie:

- ↗ Pressemitteilung
- ↗ Angemessenheitsbeschluss ((EU)2016/1250 der Kommission vom 12. Juli 2016)
- ↗ Anhänge/Annex
- ↗ FAQ
- ↗ Factsheet
- ↗ Mitteilung
- Die Kommission hat für EU-Bürger einen ↗ Leitfaden zur Erläuterung der Rechtsbehelfe bei Datenschutzverstößen veröffentlicht.

Information

Materialien zum Privacy Shield finden Sie unter Punkt 7.2.

4.4 Verbindliche Unternehmensregelungen (»Binding Corporate Rules«)

Als »ausreichende Garantien«[5] für die von einer Datenübermittlung Betroffenen können auch verbindliche Unternehmensrichtlinien dienen. Sie regeln die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten innerhalb internationaler Konzerne. Durch solche »Binding Corporate Rules« (BCR) (bislang auch »Codes of Conduct« genannt) werden Datenschutzgrundsätze für den Umgang mit personenbezogenen Daten, insbesondere Daten von Kunden, Aktionären und Mitarbeitern sowie Vertrags- oder Geschäftspartnern verbindlich und allgemein festgelegt.

Binding Corporate Rules haben den Kernprinzipien der europäischen Datenschutzrichtlinie (DS-RL) zu entsprechen und somit ein »angemessenes Schutzniveau« zu gewährleisten. Was dies konkret in Bezug auf Binding Corporate Rules bedeutet, hat die Art. 29-Datenschutzgruppe entwickelt und in mehreren Dokumenten beschrieben.

Die inhaltlichen Anforderungen an BCR hat sie insbesondere in den Arbeitspapieren 74 und 108 niedergelegt. Das Arbeitspapier 153 enthält darüber hinaus eine empfehlenswerte Checkliste mit Hinweisen, welche Anforderungen innerhalb oder außerhalb der BCR erfüllt werden müssen bzw. können.

5 Eingehend hierzu Filip »Binding Corporate Rules (BCR) aus der Sicht einer Datenschutzaufsichtsbehörde« in ZD 2013 S. 51, 54.

Die Art. 29-Datenschutzgruppe hat auch Verfahrensregelungen für die Prüfung der BCR durch die Aufsichtsbehörden erlassen. Das Arbeitspapier 133 enthält ein Formblatt zur Bestimmung der »lead authority«, die den Abstimmungsprozess der involvierten Aufsichtsbehörden koordinieren soll. Ursprünglich mussten alle nationalen Aufsichtsbehörden, aus deren Land ein Unternehmen Daten in ein Drittland übermitteln wollte, einzeln angeschrieben und um eine Stellungnahme gebeten werden. Dieses Verfahren hat sich bei mehreren zu involvierden Aufsichtsbehörden als mühsam und zeitaufwendig erwiesen. Deshalb hat man das Verfahren der gegenseitigen Anerkennung (»mutual recognition«) entwickelt. Danach erstellt die »lead authority« gemeinsam mit bis zu zwei weiteren Aufsichtsbehörden eine Stellungnahme, die (zumindest) von den an dem mutual recognition Verfahren teilnehmenden Aufsichtsbehörden anerkannt wird. Derzeit beteiligen sich 21 Länder aus dem Europäischen Wirtschaftsraum an dem Verfahren der gegenseitigen Anerkennung.

Auf der Website der Europäischen Kommission findet man ↗ allgemeine Informationen zu BCR sowie Links zu den genannten Dokumenten der Art. 29-Datenschutzgruppe.

4.4.1 Genehmigung der Binding Corporate Rules

Auf die Frage, ob die Binding Corporate Rules Gegenstand einer Genehmigung durch die Aufsichtsbehörde sein können oder müssen, gibt weder die EU-Datenschutzrichtlinie noch das BDSG eine eindeutige Antwort. Die europäische Datenschutzgrundverordnung (DS-GVO) geht von einer Genehmigungspflicht durch die Aufsichtsbehörden aus. Auch wenn nicht sicher ist, ob die von den Aufsichtsbehörden der Länder bislang vertretenen Rechtsauffassungen angesichts dieser Entwicklungen weiterhin vertreten werden, sollen sie bis zum Zeitpunkt der Anwendung der DS-GVO im Mai 2018 hier erwähnt werden.

Die Aufsichtsbehörden der Länder kommen bei der Einordnung von Binding Corporate Rules in die Vorschriften von BDSG und EU-DS-RL zu zwei unterschiedlichen Ergebnissen. Zum einen wird die Einordnung unter § 4 b Abs. 2 Satz 2 BDSG (vgl. auch Art. 25 Abs. 1 EU-DS-RL) vertreten. Da die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle trage (§ 4 b Abs. 5 BDSG), sei es Aufgabe dieser Stelle, selbst die Angemessenheit des Schutzniveaus beim Empfänger zu beurteilen; für eine Genehmigung durch die Aufsichtsbehörde fehle insoweit die Rechtsgrundlage. Dies hätte eine genehmigungsfreie Datenübermittlung zur Folge.

Dem entgegengesetzt wird die Einordnung unter § 4 c Abs. 2 BDSG vertreten (vgl. auch Art. 26 Abs. 2 EU-DS-RL). Als Argument hierfür wird der Wortlaut des § 4 c Abs. 2 BDSG sowie die Behandlung dieser Frage durch die EU-Kommission angeführt. Diese Ansicht hat zur Konsequenz, dass die Binding Corporate Rules die Grundlage für eine hiernach zu beantragende Genehmigung zur Datenübermittlung bilden. Eine Genehmigung der zuständigen Aufsichtsbehörde sei also erforderlich. Diese Auffassung wird zurzeit von den Aufsichtsbehörden in Brandenburg, Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein vertreten.

Als weitere Variante wird von einigen Aufsichtsbehörden die Auffassung vertreten, dass neben oder an Stelle der Bindung Corporate Rules die einzelnen Übermittlungen oder gleichartigen Fälle von Übermittlungen genehmigungspflichtig seien.

Die Art. 29-Datenschutzgruppe hat mit dem Arbeitspapier 108 eine Checkliste für die Zulassung von bindenden Unternehmensrichtlinien international tätiger Unternehmen entwickelt. Anhand derer können die entworfenen Unternehmensregelungen daraufhin überprüft werden, ob sie den Vorgaben der Datenschutzrichtlinie entsprechen und Regelungen über Entschädigungen für Betroffene für den Fall der Verletzung von datenschutzrechtlichen Vorschriften enthalten.[6]

Der nachfolgende Absatz beschreibt die bisherige Praxis nach dem BDSG und der DS-RL auf nationaler Ebene. Ob und inwiefern sie bis zur Anwendung der DS-GVO weiterhin so gelebt wird, ist unklar. Sofern eine Genehmigungspflicht bejaht wird, sieht die Praxis wie folgt aus:

Legt ein Unternehmen Binding Corporate Rules zur Genehmigung vor, werden diese von der zuständigen Aufsichtsbehörde in die AG »Internationaler Datenverkehr« des Düsseldorfer Kreises (gemeinsames Gremium der Landesaufsichtsbehörden) eingebracht. Dort wird eine inhaltliche Überprüfung vorgenommen und die Binding Corporate Rules werden ggf. einvernehmlich akzeptiert. Federführend bei den Beratungen ist die (z. B. nach der Hauptniederlassung des Unternehmens) zuständige Aufsichtsbehörde. Das Unternehmen kann anschließend, sofern die jeweils zuständige Aufsichtsbehörde dies für erforderlich hält, auf der Grundlage der Binding Corporate Rules die Genehmigung der konkreten Datenübermittlung bzw. gleichartigen Übermittlungsfälle stellen. Wegen des Streits über die Genehmigungspflicht ergeht in der Regel kein formeller Beschluss des Düsseldorfer Kreises, sondern es bleibt der für die einzelnen Unternehmen zuständigen Aufsichtsbehörde im Einzelfall überlassen, ob sie die Binding Corporate Rules nach § 4 c BDSG formell genehmigt oder sie ohne formelle Genehmigung als Grundlage für ein angemessenes Datenschutzniveau nach § 4 b BDSG anerkennt.

Wichtig ist, dass man sich darüber im Klaren ist, das BCR »nur« geeignete Garantien für die Absicherung des Datentransfers in ein »unsicheres Drittland« darstellen, so dass im Übrigen die allgemeinen Regelungen stets beachtet werden müssen. Das bedeutet, dass ein Datentransfer in jedem Fall einer legitimierenden Grundlage bedarf, z. B. aus § 28 Abs. 1 Nr. 2 BDSG. Des Weiteren ist im Falle einer Auftragsdatenverarbeitung auch innerhalb eines Konzerns ein ADV abzuschließen.

4.4.2 Abstimmung der Binding Corporate Rules in der EU

Angesichts der unterschiedlichen Handhabung und unklaren Rechtslage sollte rechtzeitig vor einer geplanten Übermittlung Rücksprache mit der zuständigen Aufsichtsbehörde gehalten werden!

6 vgl. dazu auch Datenschutz-Berater, DSB 7+8/2005, Drittländertransfer mit bindenden Unternehmensrichtlinien, Seite 5.

Exkurs: Binding Corporate Rules nach der DS-GVO

Die DS-GVO erkennt BCR bzw. »verbindliche interne Datenschutzvorschriften« – so die offizielle deutschsprachige Bezeichnung – ausdrücklich als »geeignete Garantien« für Datentransfers in Länder ohne angemessenes Schutzniveau an, Art. 46 Abs. 2 Buchstabe b DS-GVO. Auch wenn damit der in Rechtslehre und Rechtspraxis bekannte Begriff der BCR von der DS-GVO übernommen wurde, ist der Kreis der möglichen Nutzer deutlich erweitert worden. Waren BCR bislang auf eine Unternehmensgruppe (Konzern) fokussiert, stehen BCR nach der DS-GVO auch Gruppen von Unternehmen offen, die eine gemeinsame Wirtschaftstätigkeit ausüben, Art. 4 Abs. 20 DS-GVO. Dies kann beispielsweise ein SaaS-Anbieter mit seinen Partnern sein. BCR stellen »geeignete Garantien« für Datentransfers in Länder ohne angemessenes Schutzniveau dar, so dass es keiner – weiteren – Genehmigung für einzelne Datentransfers bedarf.

Die inhaltlichen Anforderungen von BCR sind in Art. 47 DS-GVO niedergelegt. Sie entsprechen weitgehend den bisherigen von der Art. 29-Datenschutzgruppe festgelegten Anforderungen.

Die DS-GVO schreibt vor, dass BCR im Kohärenzverfahren zu genehmigen sind, Art. 47 Abs. 1 und Art. 64 Abs. 1 Buchstabe f DS-GVO. Hierdurch soll gewährleistet werden, dass die europäischen Aufsichtsbehörden aufgrund eines gemeinsamen Verständnisses eine Stellungnahme abgeben und so einen Beitrag zur einheitlichen Anwendung der DS-GVO leisten. Die Erfahrungen mit Genehmigungen unter der Geltung der DS-RL und die unterschiedlichen mitgliedstaatlichen Vorgehensweisen haben dazu geführt, dass gesetzliche Fristen für die Vorlage von Stellungnahmen gemacht werden und dass »Schweigen als Zustimmung« gewertet wird.

Erfreulicherweise wird in Art. 46 Abs. 5 DS-GVO klargestellt, dass die von Aufsichtsbehörden auf der Grundlage von Art. 26 Abs. 2 DS-RL erteilten Genehmigungen so lange gültig bleiben, bis sie aufgehoben werden. (Alt-) BCR bleiben also auch nach mit dem Zeitpunkt der Anwendbarkeit der DS-GVO im Mai 2018 gültig. Legt ein Unternehmen seine an die Anforderungen der DS-GVO geänderten BCR der Aufsichtsbehörde vor, stellt dies keinen Antrag auf Genehmigung von (neuen) BCR dar, sondern lediglich die gemäß Art. 47 Abs. 2 Buchstabe k DS-GVO geforderte Meldung von Änderungen an den BCR.

5 Funktion einer Betriebsvereinbarung

5 Funktion einer Betriebsvereinbarung

Das Betriebsverfassungsgesetz verpflichtet sowohl den Arbeitgeber als auch den Betriebsrat, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern (§ 75 Abs. 2 BetrVG). Entsprechende Regelungen werden i.d.R. in Form von Betriebsvereinbarungen zwischen Betriebsrat und Arbeitgeber festgelegt. Sie richten sich nach den Vorgaben des § 77 BetrVG. Die getroffenen Regelungen sind grundsätzlich verbindlich für alle Arbeitnehmer des Betriebs mit Ausnahme der leitenden Angestellten. Die Durchführung obliegt dem Arbeitgeber. Eine Betriebsvereinbarung kann zum einen die datenschutzrechtlich erforderliche Zulässigkeitsnorm für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten darstellen. Sie gilt insofern als »andere Rechtsvorschrift« im Sinne des § 4 BDSG. Zum anderen kann eine Betriebsvereinbarung die mitbestimmungsrechtliche Voraussetzung für die Einführung und Anwendung von technischen Einrichtungen bilden, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Nr. 6 BetrVG).

Insgesamt stellt die Einhaltung der Beteiligungsrechte der Mitarbeitervertretung eine zwingende Wirksamkeits- und Rechtmäßigkeitsvoraussetzung dar. Ihre Nichtbeachtung führt zur Unrechtmäßigkeit der Datenverarbeitung und löst Korrekturansprüche sowohl auf Seiten der betroffenen Beschäftigten als auch seitens der betrieblichen Interessenvertretungen aus. Fraglich ist jedoch das Maß, in dem einzelne Regelungen in Betriebsvereinbarungen von den Schutzbestimmungen des BDSG abweichen dürfen: Als unstrittig gilt zunächst, dass die Betriebsvereinbarungen die Normen zwingenden Rechts einhalten müssen sowie sich an den grundgesetzlichen Werten auszurichten haben. Datenschutzrechtlich ist weiterhin ein Interessenausgleich zwischen Arbeitgeber- und Arbeitnehmerinteressen nach billigem Ermessen durchzuführen. Pauschalermächtigungen scheiden somit als Bestimmungen ebenfalls aus.[7]

Nach verbreiteter Auffassung der Aufsichtsbehörden können Betriebsvereinbarungen nur soweit vom BDSG abweichen, wie sie die dort getroffenen Regelungen durch Schutzvorkehrungen ersetzen, die den besonderen Beschäftigungsbedingungen besser angepasst, allerdings mindestens so weitreichend, sind.[8]

In der Praxis muss daher zunächst eine Beziehung zum Arbeitsverhältnis gegeben sein. Der Arbeitgeber muss weiterhin ein objektiv gerechtfertigtes Interesse haben, wobei die Interessen des Arbeitnehmers nicht in unangemessenem Maße unberücksichtigt bleiben dürfen. Ein Abweichen von den Regelungen des BDSG kann insbesondere dann als vertretbar gelten, wenn ein objektives Interesse der Arbeitnehmer an der Datenverarbeitung besteht.

Bezüglich der Übermittlung von Arbeitnehmerdaten in das Ausland stehen die Aufsichtsbehörden im Übrigen auf dem Standpunkt, dass in ihrer Wirkung auf Deutschland beschränkte Betriebsvereinbarungen zwar im Rahmen der §§ 28-30 BDSG Bedeutung haben können, aber i.d.R. nicht geeignet seien, zur Sicherstellung eines angemessenen Schutzniveaus im Ausland beizutragen.

7 BAG, Urteil vom 22.10.1986 – 5 AZR 660/85; Gola/Wronka: Handbuch zum Arbeitnehmerdatenschutz, 3. Auflage, Frechen, 2004, RdNr. 54.

8 vgl. z. B. Hamburgischer Datenschutzbeauftragter, Tätigkeitsbericht 2000/01, S. 193.

6 Konzerninterne Datenübermittlung

6 Konzerninterne Datenübermittlung

6.1 Allgemeines

Durch die Tendenz zur konzerninternen Zentralisierung von Verwaltungsdienstleistungen gerade auch im Personalbereich gewinnt die Übermittlung von Personaldaten im Konzern zunehmend an Bedeutung.

Datenschutzrechtlich hat der Gesetzgeber anders als in anderen Gebieten wie dem Steuerrecht bewusst auf ein Konzernprivileg verzichtet. Dies hat zur Folge, dass sich die Übermittlung von personenbezogenen Daten über die Grenzen rechtlich selbständiger Unternehmen hinweg an den Vorschriften des Bundesdatenschutzgesetzes, insbesondere den §§ 4, 11 und 28 BDSG auszurichten hat. Dies gilt auch dann, wenn sowohl das übermittelnde Unternehmen als auch das empfangene Unternehmen Teil des gleichen Konzern sind.

Exkurs: Ausblick auf die DS-GVO

Die EU DS-GVO hat eine solche Privilegierung für den konzerninternen Datenaustausch unter bestimmten Voraussetzungen nunmehr ausdrücklich anerkannt. Relevanter Erlaubnistatbestand dürfte hier Artikel 6 Absatz 1 Buchst. f) DS-GVO sein. Danach ist die Verwendung personenbezogener Daten zulässig, wenn »die Verarbeitung zur Wahrung der berechtigten Interessen der Verantwortlichen erforderlich ist« und kein schutzwürdiges Interesse am Ausschluss überwiegt. Erwägungsgrund 48 der DS-GVO erkennt in diesem Zusammenhang das berechtigte Interesse am konzerninternen Datenaustausch ausdrücklich an.

Konkrete Voraussetzungen und Kriterien im Einzelfall werden – bestenfalls – durch Aufsichtsbehörden und im – schlechteren Fall – durch Rechtsprechung zu bestimmen sein.

6.2 Auftragsdatenverarbeitung zwischen Konzernunternehmen

Erfolgt die Verarbeitung von Daten innerhalb von Konzernunternehmen im Auftrag und strikt nach der Weisung des beauftragenden Konzernunternehmens, so gelten die allgemeinen Regeln über die Auftragsdatenverarbeitung, wie sie in diesem Leitfaden bereits dargelegt wurden. Es bedarf für die Übermittlung der Daten und die Verwendung keiner speziellen Erlaubnis oder einer Einwilligung. Dies gilt auch, wenn eines der beteiligten Konzernunternehmen in der EU oder im ERW tätig ist.

Da die Auftragsdatenverarbeitung an Voraussetzungen wie kein Ermessenspielraum des Datenempfängers oder kein eigene Rechtsbeziehung zum Betroffenen geknüpft ist, ist eine konzernweite Datenverwendung auf der Grundlage einer Auftragsdatenverarbeitung insbesondere in den Fällen problematisch, in denen zentrale Konzernstellen eigenständig entscheiden und gespeicherte Daten anderen Konzernunternehmen zugänglich machen wollen. Hier liegen dann unter Umständen die Voraussetzungen einer ADV nicht (mehr) vor und es sind die Voraussetzungen einer Übermittlung zu prüfen.

Hierdurch entsteht ein gewisser Gestaltungsspielraum für die Konzernunternehmen.[9]

Information

Bitkom hat zur Auftragsdatenverarbeitung eine Mustervertragsanlage formuliert, die ↗ hier abgerufen werden kann. Diese Dokumente werden derzeit an die Anforderungen der Datenschutz-Grundverordnung angepasst.

6.3 Zulässigkeitsnormen für die Übermittlung

Die Übermittlung personenbezogener Daten ist nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG).

6.3.1 Einwilligung

Die Einwilligung scheidet i.d.R. als Rechtsgrundlage aus. Ihre Wirksamkeit unterliegt zum einen der notwendigen Unabhängigkeit des Betroffenen als Voraussetzung einer freien Entscheidung, was im Abhängigkeitsverhältnis zwischen Arbeitnehmer und Arbeitgeber regelmäßig angezweifelt werden kann.[10] Zum anderen ist die Einwilligung widerrufbar, was wesentliche organisatorische Einschränkungen in der Gestaltung der Übermittlungsprozesse mit sich bringen würde. Einwilligungen sind allenfalls dann denkbar, wenn auch dem Arbeitnehmer ein eindeutiger Vorteil aus der Einwilligung entsteht (z. B. bei der Teilnahme an Aktienoptionsprogrammen).

9 Vgl. ebd.

10 Däubler: Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle, 4. Auflage, Frankfurt, M., 2002, RdNr. 135ff; Gola/Wronka: Handbuch zum Arbeitnehmerdatenschutz, 3. Auflage, Frechen, 2004, RdNr. 145ff.

6.3.2 § 28 BDSG als Erlaubnistatbestand

Als Erlaubnistatbestände des BDSG kommen § 28 Abs. 1 Satz 1 Nr. 1 sowie § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 3 Nr. 1 in Betracht.

Die Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 BDSG setzt zunächst das Vorhandensein eines (Arbeits-) Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses (z. B. in Bewerbungssituationen) zwischen dem Betroffenen und der verantwortlichen Stelle voraus. Im Verhältnis zu Konzernunternehmen, die nicht gleichzeitig Arbeitgeber des Betroffenen sind ist dies z. B. dann gegeben, wenn ein konzerndimensionales Arbeitsverhältnis vorliegt (z. B. bei Führungskräften, die sich verpflichtet haben, bei Bedarf in anderen Gesellschaften zu arbeiten).

Darüber hinaus lässt sich die Notwendigkeit der Datenübermittlung durch den Arbeitgeber an ein anderes Konzernunternehmen im Rahmen des Arbeitsvertragszwecks dadurch rechtfertigen, dass einzelne Funktionen für den Mitarbeiter transparent und klar abgegrenzt an andere Konzernunternehmen übertragen werden.

In Anwendung der § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 3 Satz 1 Nr. 1 BDSG ist zunächst die Vorgabe des Gesetzgebers zu berücksichtigen, der explizit auf die Einführung eines Konzernprivilegs verzichtet hat.

Hingegen ist nach Auffassung der Aufsichtsbehörden für den nicht-öffentlichen Bereich eine Übermittlung als zulässig zu betrachten, »wenn die beteiligten Konzernunternehmen besondere Maßnahmen zugunsten der Arbeitnehmer treffen, so dass das Ergebnis der Abwägung doch noch zugunsten der berechtigten Interessen der Konzernunternehmen ausfällt.«[11] Hierzu gehören z. B. die Schaffung eines konzernweiten Datenschutzkonzepts sowie Maßnahmen zu Sicherstellung von Transparenz und Betroffenenrechten. Diese Regelungen sind sowohl zwischen den beteiligten Konzernunternehmen als auch im Verhältnis zu den Arbeitnehmern verbindlich zu vereinbaren.

6.3.3 Die Betriebsvereinbarung als Erlaubnistatbestand

Auch eine Betriebsvereinbarung als andere Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG kommt als Erlaubnistatbestand für eine Übermittlung in Betracht. Hierbei ist der Regelungsspielraum jedoch begrenzt (vgl. Kapitel 5).

11 Arbeitsbericht der ad-hoc-Arbeitsgruppe »Konzerninterner Datentransfer« des »Düsseldorfer Kreises«, veröffentlicht durch das Regierungspräsidium Darmstadt, 2005.

7 Begriffsbestimmungen, Materialien, Grafiken und Übersichten

7 Begriffsbestimmungen, Materialien, Grafiken und Übersichten

7.1 Begriffsbestimmungen

Im Folgenden werden einige zentrale Begriffe des Datenschutzes kurz erläutert:

- **Automatisierte Verarbeitung**
  Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

- **Besondere Arten personenbezogener Daten**
  Nach § 3 Abs. 9 BDSG sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeiten, Gesundheit oder Sexualleben »besondere Arten personenbezogener Daten« (häufig auch als »sensitive Daten« bezeichnet).

- **Betroffener**
  Betroffener ist die natürliche Person, deren Daten erhoben bzw. verarbeitet werden.

- **Datei mit personenbezogenen Daten bzw. nicht automatisierte Datei**
  Eine Datei ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geographischen Gesichtspunkten aufgeteilt geführt wird.

- **Datenexporteur**
  Datenexporteur ist der für die Verarbeitung Verantwortliche, der personenbezogene Daten übermittelt.

- **Datenimporteur**
  Datenimporteur ist der für die Verarbeitung Verantwortliche, der sich bereit erklärt, vom Datenexporteur personenbezogene Daten für die Verarbeitung entgegenzunehmen.

- **Dritter**
  Dritter ist jede Stelle außerder betroffenen Person,dem für die Verarbeitung Verantwortlichen und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen befugt sind, die Daten zu verarbeiten. Nicht unter den Begriff »Dritter« fallen rechtlich unselbstständige Zweigstellen eines Unternehmens (wie z. B. Filialen). Rechtlich selbstständige Einrichtungen – wie Betriebskrankenkassen – sind jedoch auch dann Dritte, wenn sie organisatorisch, räumlich oder personell mit der speichernden Stelle verbunden sind.

- **Drittland**
  Als Drittländer werden alle anderen Staaten außerhalb der EU bzw. des EWR gesehen.

- **Einwilligung**
  Einwilligung ist jede Willensbekundung, die ohne Zwang für den konkreten Fall und in Kenntnis der Sachlage erfolgt. Mit der Einwilligung akzeptiert die betroffene Person, dass personenbezogene Daten, die sie betreffen, verarbeitet werden.

- **EWR (häufig auch EWG genannt)**
  Europäischer Wirtschaftsraum (häufig auch EWG genannt). Er umfasst die Länder der EU, sowie die drei EFTA-Staaten Norwegen, Liechtenstein und Island.

- **Empfänger**
  Empfänger ist jede Stelle, die Daten erhält.

- **Messaging-Dienste**
  Instant Messaging ist ein Dienst, der es erlaubt, sich in Echtzeit über das Internet zu unterhalten oder kurze Nachrichten an andere Teilnehmer zu schicken oder diesen kleinere Dateien zukommen zu lassen.

- **Nutzen von Daten**
  Jede Verwendung außer Verarbeitung (z. B. Duplizieren oder Kopieren von Daten, Erstellung personenbezogener Auswertungen).

- **Personenbezogene Daten**
  Personenbezogene Daten sind Einzelangaben über persönliche Verhältnisse (z. B. Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Berufs- und Branchenbezeichnung, Zeugnisnoten, Beurteilungen, Krankheiten, Vorstrafen) oder sachliche Verhältnisse (z. B. Einkommen, Besitzverhältnisse, Steuern, Versicherungen, Vertragskonditionen) einer bestimmten oder bestimmbaren natürlichen Person. Als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, wirtschaftlichen, kulturellen oder sozialen Identität sind. Geschützt sind also alle Informationen über die einzelne natürliche Person, aber nicht über juristische Personen (AG, GmbH, e.V. etc.).

- **Übermitteln**
  Übermitteln ist die Bekanntgabe von Daten aus einer Datei an Dritte durch aktive Weitergabe in jeglicher Form (mündlich, schriftlich, versenden usw.) oder durch Bereithalten der Daten zur Einsichtnahme oder zum Abruf. Bei automatisierten Abrufverfahren liegt ein Übermitteln nach dem BDSG erst dann vor, wenn der Dritte die Daten einsieht (Lesen oder Betrachten) oder abruft (z. B. Sichtbarmachung der Daten auf seinem Monitor).

- **Verantwortliche Stelle**
  Verantwortliche Stelle ist die Stelle, die eine Verarbeitung selbst durchführt oder durch andere im Auftrag durchführen lässt.

- **Verarbeitung personenbezogener Daten**
  Verarbeitung ist jeder Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Wiederauffinden, das Abfragen, die Weitergabe durch Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten von personenbezogenen Daten.

- Speichern (Erfassen, Aufnehmen, Aufbewahren)
- Verändern (inhaltliches Umgestalten)
- Übermitteln (Bekanntgabe, Weitergabe, Einsichtnahme, Abrufen)
- Sperren (Kennzeichnung zur Verarbeitungs- und Nutzungseinschränkung)
- Löschen (Unkenntlichmachung)

7.2 Materialien zum EU-US Privacy Shield

7.2.1 Die Privacy Shield Principles

Informationspflicht

Die Organisation muss Privatpersonen über Folgendes informieren:

- ihre Teilnahme am Datenschutzschild mit einem Link zur Datenschutzschild-Liste oder der Webanschrift der Liste,
- die Arten der erfassten personenbezogenen Daten und gegebenenfalls die Einrichtungen oder Tochterunternehmen der Organisation, die die Grundsätze ebenfalls einhalten,
- ihre Verpflichtung, die Grundsätze auf alle aus der EU empfangenen personenbezogenen Daten unter Zugrundelegung des Datenschutzschilds anzuwenden,
- zu welchem Zweck sie die personenbezogenen Daten über sie erhebt und verwendet,
- wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, wozu auch Angaben zu einer relevanten Einrichtung in der EU gehören, die auf derartige Nachfragen oder Beschwerden eingehen kann,
- die Kategorie und Identität von Dritten, an die die Daten weitergegeben werden, sowie der Zweck der Weitergabe,
- das Recht von Privatpersonen auf Zugang zu ihren personenbezogenen Daten,
- welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe ihrer personenbezogenen Daten einzuschränken,

- das zur Bearbeitung von Beschwerden und für einen kostenlosen Rechtsschutz für die Privatperson benannte unabhängige Streitbeilegungsgremium, und ob es sich 1) um das von Datenschutzbehörden eingerichtete Gremium, 2) um einen in der EU ansässigen Anbieter für alternative Streitbeilegung oder 3) um einen in den Vereinigten Staaten ansässigen Anbieter für alternative Streitbeilegung handelt,
- die für die Organisation geltenden Ermittlungs- und Durchsetzungsbefugnisse der FTC, des Verkehrsministeriums oder einer anderen bevollmächtigten US-Behörde,
- die Möglichkeit, unter bestimmten Bedingungen ein verbindliches Schiedsverfahren anzustrengen,
- die Bestimmung, personenbezogene Daten auf rechtmäßige Anfrage von Behörden offenzulegen, um Erfordernissen der nationalen Sicherheit oder der Strafverfolgung nachzukommen, und
- die Haftung der Organisation bei Weitergabe an Dritte.

Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig ersucht werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Wahlmöglichkeit

Die Organisation muss Privatpersonen die Möglichkeit geben zu wählen (»Opt-out«), ob ihre personenbezogenen Daten i) an Dritte weitergegeben werden sollen oder ii) für einen Zweck verwendet werden sollen, der sich von dem ursprünglichen oder dem nachträglich von der betreffenden Person genehmigten Erhebungszweck wesentlich unterscheidet. Der betroffenen Person muss die Ausübung ihres Wahlrechts durch leicht erkennbare, verständliche und leicht zugängliche Verfahren ermöglicht werden.

Abweichend vom vorstehenden Absatz unterliegt die Übermittlung solcher Daten an einen Dritten nicht dem Grundsatz der Wahlmöglichkeit, wenn dieser im Auftrag oder auf Anweisung der Organisation tätig ist. Die Organisation schließt jedoch stets einen Vertrag mit dem Beauftragten.

Bei sensiblen Daten (d. h. Angaben über den Gesundheitszustand, über Rassen- oder ethnische Zugehörigkeit, über politische, religiöse oder weltanschauliche Überzeugungen, über die Mitgliedschaft in einer Gewerkschaft oder über das Sexualleben) benötigen die Organisationen die ausdrückliche Zustimmung (»Opt-in«) der betroffenen Personen, wenn diese Daten i) an Dritte weitergegeben oder ii) für einen anderen als den ursprünglichen Erhebungszweck oder den Zweck verwendet werden sollen, dem die betroffene Person nachträglich durch Ausübung des Wahlrechts zugestimmt hat. Darüber hinaus sollen die Organisationen alle ihnen von Dritten übermittelten personenbezogenen Daten als sensibel behandeln, die der Übermittler als sensibel einstuft und behandelt.

Verantwortlichkeit für Weitergabe

Eine Organisation darf personenbezogene Daten nur dann an Dritte, die als für die Verarbeitung Verantwortliche tätig sind, weitergeben, wenn sie die Grundsätze der Informationspflicht und der Wahlmöglichkeit anwendet. Die Organisation muss auch einen Vertrag mit dem als für die Verarbeitung Verantwortlichen tätigen Dritten schließen, in dem festgelegt ist, dass diese Daten nur in begrenztem Rahmen für bestimmte Zwecke im Einklang mit der von der betroffenen Person erteilten Zustimmung verarbeitet werden dürfen und dass der Empfänger das gleiche Schutzniveau vorsieht wie die Grundsätze und er die Organisation entsprechend unterrichten muss, wenn er feststellt, dass er diese Verpflichtung nicht mehr erfüllen kann. Der Vertrag muss festlegen, dass im Falle einer derartigen Festlegung der als Verantwortlicher tätige Dritte die Verarbeitung einstellt oder mit anderen sinnvollen und geeigneten Maßnahmen Abhilfe schafft.

Bei der Weitergabe von personenbezogenen Daten an einen Dritten, der in ihrem Auftrag und auf ihre Anweisung tätig ist, gilt für eine Organisation Folgendes: i) sie darf diese Daten nur in begrenztem Rahmen für bestimmte Zwecke weitergeben; ii) sie muss sich vergewissern, dass der Beauftragte verpflichtet ist, zumindest das Maß an Schutz personenbezogener Daten zu gewährleisten, das in den Grundsätzen gefordert wird; iii) sie muss mit angemessenen und geeigneten Schritten sicherstellen, dass der Beauftragte die weitergegebenen personenbezogenen Daten in einer den Verpflichtungen der Organisation im Rahmen der Grundsätze konformen Weise verarbeitet; iv) sie muss vom Beauftragten verlangen, dass er sie unterrichtet, wenn er feststellt, dass er seine Verpflichtung, das gleiche Schutzniveau vorzusehen wie in den Grundsätzen gefordert, nicht mehr erfüllen kann, v) sie muss auf entsprechenden Hinweis, einschließlich nach iv), sinnvolle und geeignete Schritte unternehmen, um eine unbefugte Verarbeitung zu unterbinden; vi) sie muss dem Ministerium auf Verlangen eine Zusammenfassung oder ein Exemplar der einschlägigen Datenschutzbestimmungen

Sicherheit

Organisationen, die personenbezogene Daten erstellen, verwalten, verwenden oder verbreiten, müssen angemessene und geeignete Maßnahmen ergreifen, um sie vor Verlust, Missbrauch und unbefugtem Zugriff, Weitergabe, Änderung und Zerstörung zu schützen; dabei sind insbesondere die Risiken bei der Verarbeitung und die Art der personenbezogenen Daten zu berücksichtigen.

Datenintegrität und Zweckbindung

In Übereinstimmung mit den Grundsätzen müssen personenbezogene Daten auf die Informationen beschränkt sein, die für den Verarbeitungszweck erheblich sind.2 Eine Organisation darf personenbezogene Daten nicht in einer Weise verarbeiten, die mit dem ursprünglichen Erhebungszweck oder mit dem Zweck unvereinbar ist, dem der Betroffene nachträglich zugestimmt hat. In dem für diese Zwecke notwendigen Umfang muss die Organisation durch angemessene Maßnahmen gewährleisten, dass die personenbezogenen Daten für den vorgesehenen Zweck hinreichend zuverlässig, genau, vollständig und aktuell sind. Die Organisation muss die Grundsätze so lange einhalten, wie sie diese Informationen aufbewahrt.

Die Daten dürfen nur so lange in einer Form aufbewahrt werden, die eine Person identifiziert oder identifizierbar macht3, wie damit ein Verarbeitungszweck im Sinne von 5a erfüllt wird. Diese Verpflichtung hindert Organisationen nicht daran, personengebundene Informationen über längere Zeiträume zu verarbeiten, solange und soweit diese Verarbeitung hinreichend den Zwecken einer Archivierung im öffentlichen Interesse, des Journalismus, der Literatur und Kunst, der wissenschaftlichen oder historischen Forschung und der statistischen Analyse dient. In diesen Fällen unterliegt die Verarbeitung den anderen Grundsätzen und Bestimmungen der Regelung. Die Organisationen sollen zur Einhaltung dieser Bestimmung angemessene und geeignete Maßnahmen ergreifen.

Auskunftsrecht

Privatpersonen müssen Zugang zu den personenbezogenen Daten haben, die eine Organisation über sie besitzt, und sie müssen die Möglichkeit haben, diese zu korrigieren, zu ändern oder zu löschen, wenn sie falsch sind oder unter Missachtung der Grundsätze verarbeitet wurden, es sei denn, die Belastung oder die Kosten für die Gewährung des Zugangs würden in dem jeweiligen Fall in einem Missverhältnis zu den Nachteilen für den Betroffenen stehen, oder Rechte anderer Personen als des Betroffenen würden verletzt.

Rechtsschutz, Durchsetzung und Haftung

Für einen effektiven Schutz der Privatsphäre müssen belastbare Mechanismen geschaffen werden, die die Einhaltung der Grundsätze gewährleisten, Rechtsbehelfe für Betroffene vorsehen, bei deren Daten die Grundsätze nicht eingehalten wurden, sowie Sanktionen für die Organisation, die die Grundsätze nicht befolgt. Diese Mechanismen müssen mindestens Folgendes umfassen:

i. leicht zugängliche, von unabhängigen Stellen durchgeführte Verfahren, nach denen Beschwerden, die betroffene Personen unter Berufung auf die Grundsätze erhoben haben, ohne Kosten für den Betroffenen untersucht und zügig behandelt werden und nach denen Schadenersatz geleistet wird, wenn das geltende Recht oder private Regelungen dies vorsehen;

ii. Kontrollmaßnahmen, um zu überprüfen, ob die Bescheinigungen und Behauptungen der Organisationen über ihre Datenschutzmaßnahmen der Wahrheit entsprechen und ob diese Maßnahmen wie angegeben durchgeführt werden, und insbesondere in Bezug auf Verstöße;

iii. Verpflichtungen zur Lösung von Problemen, die daraus resultieren, dass Organisationen die Einhaltung der Grundsätze zwar erklärt, sich aber trotzdem nicht daran gehalten haben, sowie entsprechende Sanktionen für diese Organisationen. Die Sanktionen müssen hinreichend streng sein, um sicherzustellen, dass die Organisationen die Grundsätze einhalten.

Organisationen und die von ihnen gewählten unabhängigen Beschwerdestellen werden rasch auf Anfragen und Auskunftsbegehren des Ministeriums reagieren, die mit dem Datenschutzschild im Zusammenhang stehen.

Alle Organisationen müssen zügig auf von Behörden der EU-Mitgliedstaaten über das Ministerium weitergeleitete Beschwerden bezüglich der Einhaltung der Grundsätze reagieren. Organisationen, die sich für eine Zusammenarbeit mit Datenschutzbehörden entschieden haben, einschließlich Organisationen, die Personaldaten verarbeiten, müssen im Zusammenhang mit der Untersuchung und Bearbeitung von Beschwerden unmittelbar auf diese Behörden eingehen.

Organisationen sind verpflichtet, Ansprüche im Schiedsverfahren zu regeln und die in Anlage I aufgeführten Bedingungen einzuhalten, sofern eine Privatperson durch Benachrichtigung der betreffenden Organisation und entsprechend den Verfahren und Bedingungen nach Anlage I ein verbindliches Schiedsverfahren beantragt hat.

Im Zusammenhang mit einer Weitergabe ist eine dem Datenschutzschild angehörende Organisation für die Verarbeitung der personenbezogenen Daten, die sie im Rahmen des Datenschutzschilds erhält und anschließend an einen Dritten weitergibt, der in ihrem Auftrag und auf ihre Anweisung tätig ist, verantwortlich. Die dem Datenschutzschild angehörende Organisation bleibt nach den Grundsätzen haftbar, wenn ihr Beauftragter diese personenbezogenen Daten auf eine Art und Weise verarbeitet, die nicht im Einklang mit den Grundsätzen steht, es sei denn, sie weist nach, dass sie für das Ereignis, das den Schaden bewirkt hat, nicht verantwortlich ist.

Ist gegen eine Organisation eine Anordnung der FTC oder ein Gerichtsbeschluss wegen eines Verstoßes ergangen, macht die Organisation jene Teile eines der FTC vorgelegten Compliance- oder Sachstandsberichts, die den Datenschutzschild betreffen, öffentlich, soweit dies mit den Verpflichtungen zur Geheimhaltung im Einklang steht. Das Ministerium hat eine spezielle Kontaktstelle eingerichtet, an die sich Datenschutzbehörden bei Compliance-Problemen von dem Datenschutzschild angehörenden Organisationen wenden können. Die FTC wird Fälle der Missachtung der Grundsätze, die ihr vom Ministerium und Behörden der EU-Mitgliedstaaten zugeleitet wurden, vorrangig behandeln und vorbehaltlich der geltenden Geheimhaltungsvorschriften zeitnah mit den vorlegenden staatlichen Behörden Informationen zu diesen Fällen austauschen.

7.2.2 Zusatzgrundsätze zum Privacy Shield

1. Sensible Daten
2. Ausnahmen für den journalistischen Bereich
3. Hilfsweise Haftung
4. Due Diligence Prüfung und Wirtschaftsprüfung
5. Die Rolle der Datenschutzbehörden
6. Selbstzertifizierung
7. Anlassunabhängige Kontrolle
8. Auskunftsrecht
9. Personaldaten
10. Obligatorische Verträge bei Weitergabe
11. Beschwerdeverfahren und Durchsetzung
12. Wahlmöglichkeit – Zeitpunkt des Widerspruchs
13. Reisedaten
14. Arzneimittel und Medizinprodukte
15. Daten aus öffentlichen Registern und öffentlich zugängliche Daten

Die inhaltlichen Ausführungen sind unter Anhang 2 des Durchführungsbeschlusses 2016/1250 der Kommission zu finden und können ↗ **hier** abgerufen werden.

7.2.3 Übersicht EU-Kommission Fact Sheet

Strenge Auflagen für Unternehmen und starke Durchsetzung

- Mehr Transparenz
- Wirksame Aufsichtsmechanismen, um sicherzustellen, dass Unternehmen die Regeln einhalten
- Sanktionen und Streichung von Privacy Shield - Liste
- Strengere Bedingungen für Weitergabe von Daten durch teilnehmende Unternehmen an Dritte

Wirksamer Rechtsschutz

Verschiedene Rechtsschutzmöglichkeiten

- Direkt beim Unternehmen: Unternehmen müssen innerhalb von 45 Tagen dem Betroffenen auf die Beschwerde antworten
- Alternative Streitbeilegung: Kostenlos
- Kontrolle durch EU-Datenschutzbehörde: Diese werden mit US-Handelsministerium und Federal Trade Commission zusammenarbeiten und dafür sorgen, dass Beschwerden von Bürgerinnen und Bürgern der EU nachgegangen und abgeholfen werden
- Schiedsverfahren durch Privacy Shield Panel: Als letzte Instanz

Schutzvorkehrungen bei Datenzugriff durch US-Behörden

- Zum ersten Mal schriftliche Zusicherungen, dass jeglicher Zugriff von US-Behörden auf personenbezogene Daten strengen Anforderungen und gerichtlichen Rechtsschutz unterliegt
- Zusicherungen, dass es keinen massenhaften Zugriff auf personenbezogene Daten ohne irgendeine Differenzierung, Einschränkung oder Ausnahme gibt
- Berichte von Unternehmen, wie oft sie von US-Behörden nach Zugang zu personenbezogenen Daten angefragt wurden
- Unabhängige Ombudsstelle, an die sich Bürger mit Rechtschutzbegehren, die den Bereich der nationalen Sicherheit betreffen, wenden können

Überprüfung des Angemessenheitsbeschlusses

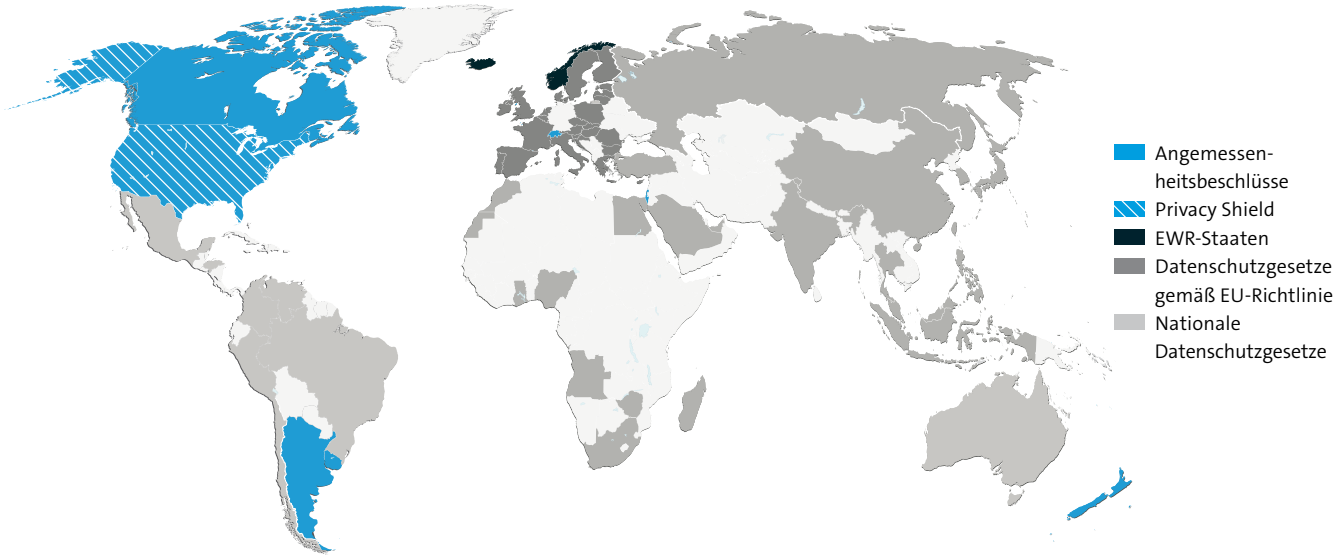
Jährliche gemeinsame Überprüfung

- Gemeinsame Überwachung der Funktionsweise des Privacy Shield und schriftlichen Zusicherungen der USA
- Von der EU-Kommission und dem US-Handelsministerium durchgeführt, an der ggf. auch Vertreter der Nachrichtendienste beteiligt werden können

Quelle: ↗ Factsheets der EU-Kommission (2016)

7.3 Übersicht über den weltweiten Stand des Datenschutzes

7.3.1 Grafische Übersicht über den weltweiten Stand des Datenschutzes



Hinweis: Eine Übersicht zu nationalen Datenschutzgesetzen finden Sie auch auf dieser ↗ Webseite von DLA Piper.

7.3.2 Erläuterung zur grafischen Übersicht über den weltweiten Stand des Datenschutzes

Stand November 2016

Datenschutz-Gesetze gemäß EU-Richtlinie 95/46/EG	EWR – Staaten
Belgien	Island
Bulgarien	Liechtenstein
Dänemark	Norwegen
Estland	
Finnland	
Frankreich	
Griechenland	
Großbritannien	
Irland	
Italien	
Kroatien	
Lettland	
Litauen	
Luxemburg	
Malta	
Niederlande	
Österreich	
Polen	
Portugal	
Rumänien	
Schweden	
Slowakei	
Slowenien	
Spanien	
Tschechien	
Ungarn	
Zypern	

Angemessenes Datenschutzniveau durch EU-Kommission anerkannt	EU-US Privacy Shield Abkommen
Argentinien	USA
Andorra	
Guernsey	
Isle of Man	
Jersey	
Kanada	
Neuseeland	
Israel	
Schweiz	
Färöer Inseln	
Uruguay	

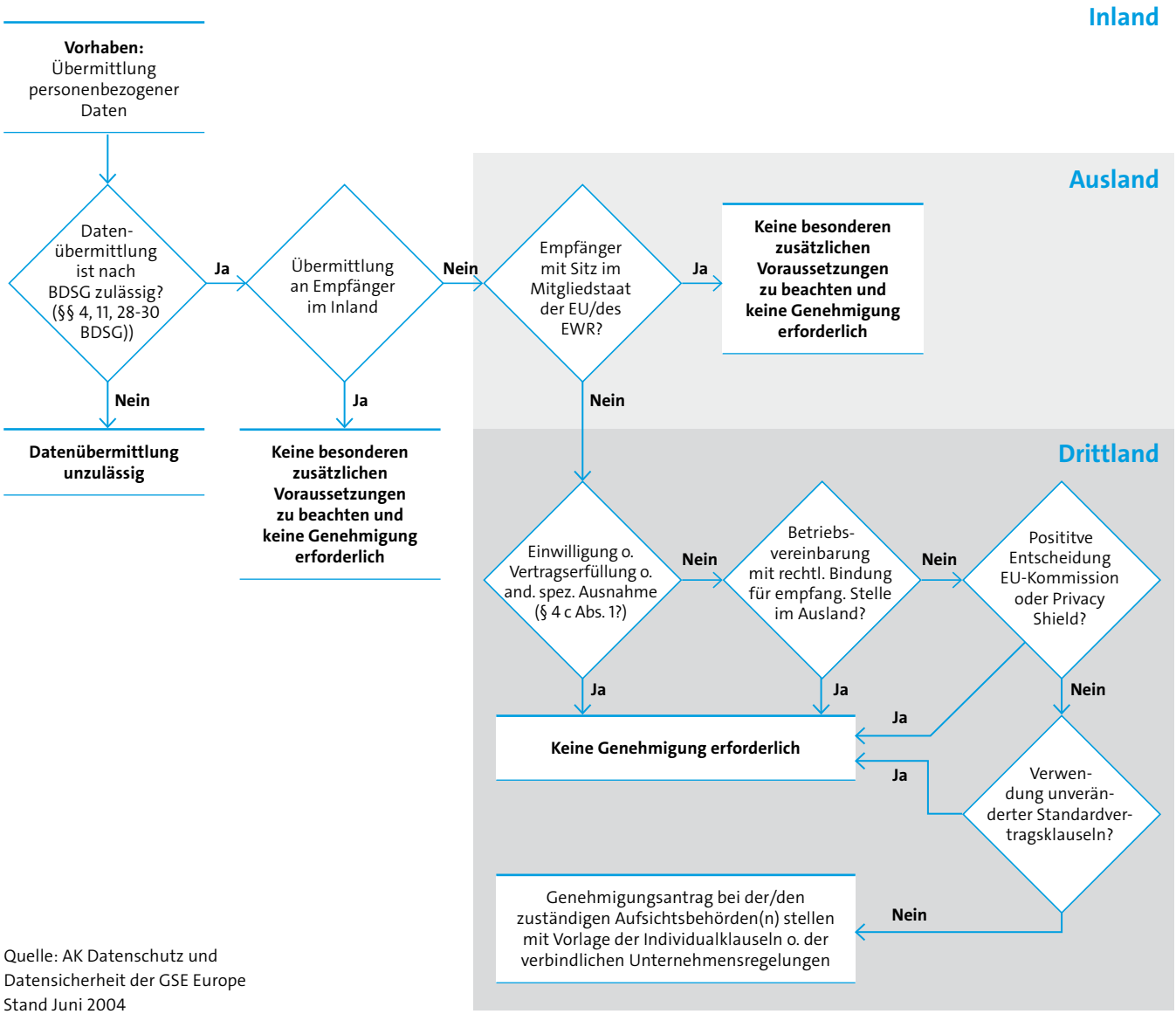
Datenschutzbehörden in Europa (außerhalb EWR)	Datenschutzbehörden International	
Albanien	Argentinien	Marokko
Bosnien und Herzegowina	Australien	Neuseeland
Georgien	Benin	Paraguay
Kosovo	Brasilien	Peru
Moldawien	Burkina Faso	Philippinen
Russland	Hong Kong	Singapur
Schweiz	Israel	Südkorea
Serbien	Japan	Senegal
Türkei	Kanada	Taiwan
Ukraine	Kap Verde	Thailand
	Kolumbien	Tunesien
	Costa Rica	Uruguay
	Côte d'Ivoire	USA
	Malaysia	
	Mali	
	Mauritius	
	Mexiko	

Quelle: International Conference of Data Protection & Privacy Commissioners (↗ ICDPPC)

Nationale Datenschutz-Gesetze	
Ägypten	Mosambik
Angola	Neuseeland
Argentinien	Nigeria
Australien	Pakistan
Brasilien	Panama
Costa Rica	Peru
Armenien	Philippinen
Belize	Russland
Bosnien Herzegowina	Saudi-Arabien
Chile	Schweiz
China	Seychellen
Ecuador	Singapur
Ghana	Serbien und Montenegro
Honduras	Südafrika
Hong Kong	Südkorea
Indien	Taiwan
Indonesien	Thailand
Israel	Trinidad und Tobago
Japan	Türkei
Kanada	Ukraine
Kolumbien	Uruguay
Madagaskar	Usbekistan
Marokko	Vereinigte Staaten
Malawi	Venezuela
Malaysia	Weißrussland
Mazedonien	Zimbabwe
Mexiko	

7.4 Entscheidungshilfe Auftragsdatenverarbeitung

Überblick über die »Zonen« eines Drittlandtransfers



Quelle: AK Datenschutz und Datensicherheit der GSE Europe
Stand Juni 2004

Die Entscheidungshilfe wurde von einer Arbeitsgruppe (M. Schmidt, V. Backes, H. Eul, M. Guthmann, R. Martwich) des Arbeitskreises Datensicherheit und Datenschutz der GSE Europe erstellt und erstmals veröffentlicht in der RDV 2004 S. 156 ff.

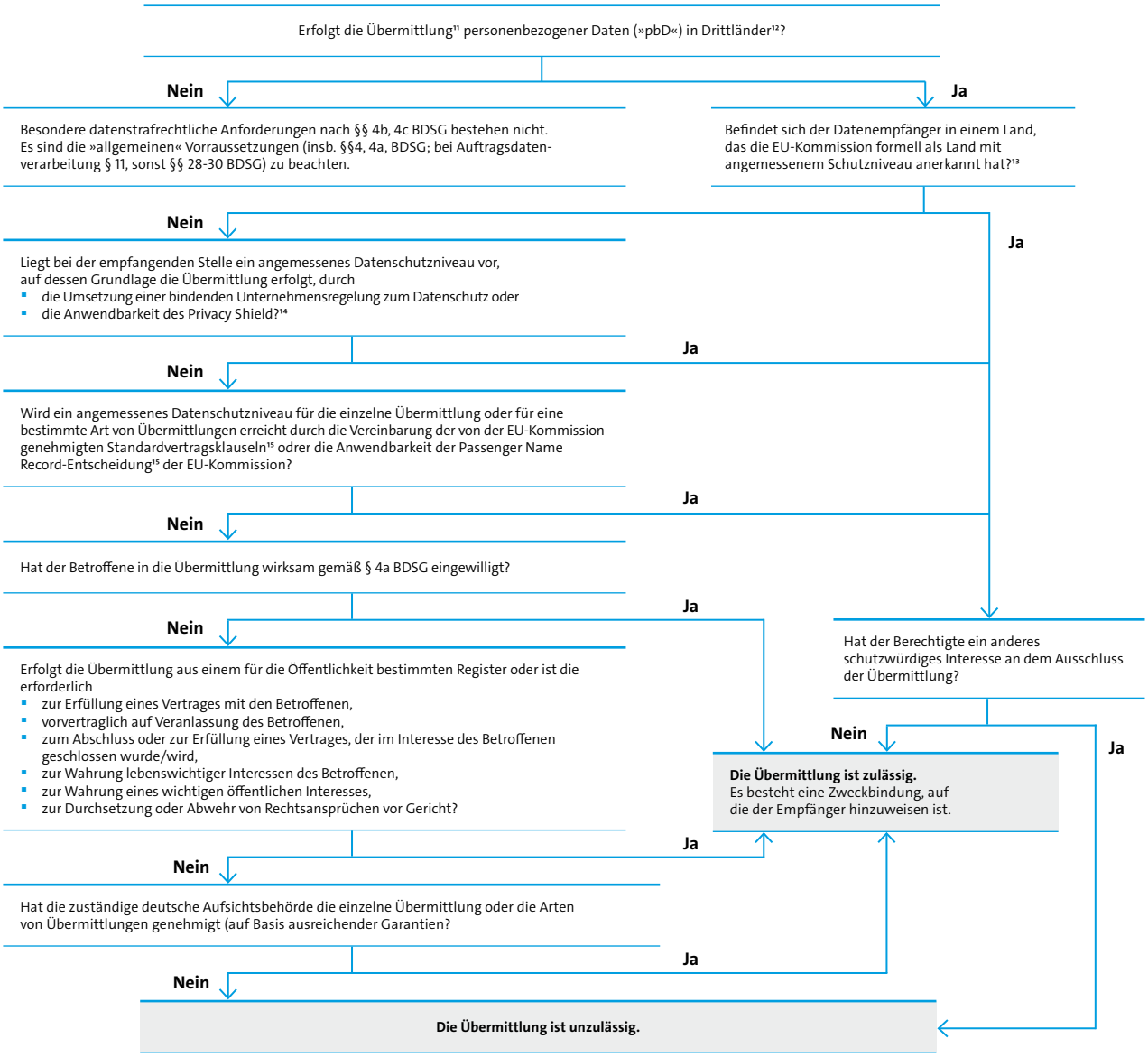
7.5 Übersicht über die rechtlichen Mögklichkeiten der Übermittlung personenbezogener Daten in Drittländer

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Pb Daten	Bemerkungen
Datenübermittlung ist zur Erfüllung des Vertrages o. zur Durchführung vorvertraglicher Maßnahmen erforderlich (§ 4 c Abs. 1 Nr. 2 BDSG)	Vertrag o. vertragsähnliche Beziehung zwischen verantwortlicher Stelle und Betroffenem	Individuell; zwischen Betroffenen und verantwortlicher Stelle	Durch Abgabe der entsprechenden Willenserklärungen von der verantwortlichen Stelle und dem Betroffenen	Grundsätzlich die pb Daten des Betroffenen, die für die Durchführung des Vertrages erforderlich sind	Keine Mitwirkung erforderlich	Vertragsbeispiele: Hotelreservierung im Ausland; Arbeitsvertrag mit ausländischem Arbeitgeber; Warenbestellung (auch online) im Ausland
Einwilligung (§ 4 c Abs. 1 Nr. 1 BDSG)	Einseitige, empfangsbedürftige Einwilligungserklärung	Individuell; zwischen Betroffenem und verantwortlicher Stelle	Durch Abgabe der entsprechenden Willenserklärung seitens des Einwilligenden	Grundsätzlich die autorisierten pb Daten des Betroffenen; Umfang im Rahmen der gesetzlichen Möglichkeiten, der guten Sitten u. des vorgesehenen Zwecks	Keine Mitwirkung erforderlich	Einwilligung muss Aussagen zum gewährleisteten o. nicht gewährleisteten Datenschutzniveau enthalten
Gesetzliche Ausnahmen (§ 4 c Abs. 1 Nr. 3-6 BDSG)	Gesetzlicher Ausnahmetatbestand	Begrenzt auf den Sachverhalt der Ausnahmeregelung	Prüfung erforderlich, ob die Voraussetzungen des Ausnahmetatbestands vorliegen	Mitarbeiter-,Kunden-, Nichtkunden, -Interessenten und Lieferantendaten, soweit für die Übermittlung im Rahmen der Ausnahmeregelung erforderlich	Keine Mitwirkung erforderlich	z. B. Wahrung eines wichtigen öffentlichen Interesses; Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht; Wahrung lebenswichtiger Interessen
Drittländer mit durch die EU Kommission festgestelltem angemessenen Datenschutzniveau (§ 4 b Abs. 3 BDSG)	Entscheidung gemäß Art. 25 Abs. 6 EU-DSRL (EU-Kommissionsentscheidung)	Gilt für alle Empfänger im entscheidungsgegenständlichen Drittland	n.a.	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten	Keine Mitwirkung erforderlich	Eine Empfehlung der Arbeitsgruppe nach Art 29 bzw. eine Kommissionsentscheidung liegen derzeit vor für: Schweiz, Canada (teilweise), Argentinien, Guernsey, Isle of Man
Individueller Datenschutz-vertrag (§4 c Abs. 2 BDSG)	Vertragliche, verbindliche Regelung zwischen den Parteien (auch mehrere, auch Unterauftragsnehmer) über den Umgang mit Personen bezogenen Daten	Zwischen den Vertragsparteien (auch mehr als 2)	Durch Abgabe der entsprechenden Willenserklärungen zwischen den vertragsschließenden Parteien	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten und Lieferantendaten soweit sie Gegenstand des individuellen Datenschutzvertrages sein sollen	Genehmigung einzelner Datenübermittlungen oder bestimmter Arten von Übermittlungen pb Daten gem. § 4 c Abs. 2 BDSG	Flexibel; je nach Umfang auch zeitaufwendig

	»Art«	Geltungsbereich	Abschluss	Pb Daten	Pb Daten	Bemerkungen
Vertrag auf Basis der Eu-Standard-vertragsklauseln für die Übermittlung Personen bezogener Daten (auch an Auftragsverarbeiter) in Drittländer (§4 c Abs. 2 BDSG)	Vertrag zwischen Datenexpoteur und Datenimpoteur auf Basis der EU-Kommissionsentscheidung zu den Standardklauseln	Zwischen Datenimpoteur(en) in einem Drittland und Expoteur (en) mit Sitz im EWR.	Durch Abgabe der entsprechenden Willenserklärungen zwischen den vertragschließenden Parteien	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten und Lieferantendaten soweit sie Gegenstand des EU-Standard-Vertrages sein sollen	Bei unverändertem Abschluss des Vertrages keine Genehmigung erforderlich. Information der Aufsichtsbehörden über den Abschluss sinnvoll. Einige Aufsichtsbehörden erwarten Vorlage der entsprechend. Verträge	Schnell umsetzbar. Einfach. Für große internationale Unternehmens-verbünde wohl unpraktikabel, da umfangreiches Vertragsmanagement erforderlich
Binding Corporate Rules (»verbindliche unternehmens-interne Vorschriften für den internationalen Datentransfer«; § 4 c Abs. 2 BDSG	Verbindliche Unternehmensregelungen (»Binding Corporate Rules«) für Teile oder die Gesamtheit eines multinationalen Unternehmensverbundes (Konzern) oder anderen Wirtschaftsgebildes, die die entsprechenden Datenschutzanforderungen definieren	Die Teile des Konzerns, für die die Unternehmensregelungen (»Binding Corporate Rules«) verbindlich sind	Verbindliche, interne Anweisung durch die führende Gesellschaft	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten soweit sie Gegenstand des Binding Corporate Rules sein sollen	Genehmigung einzelner Datenübermittlungen oder bestimmter Arten von Übermittlungen pb Daten gem. § 4 c Abs. 2 BDSG	Anforderungen siehe WP 74 der Art. 29-Datenschutzgruppe – Zur Zeit Diskussion innerhalb der Aufsichtsbehörden, ob überhaupt Genehmigung notwendig
Privacy Shield (§ 4 c Abs. 2 BDSG)	Vereinbarung zwischen den USA und der EU über verbindliche Verhaltensregeln zum Datenschutz für US-amerikanische Unternehmen	Datenverkehr pb Daten zwischen Datenexporteuren mit Sitz in der EU und an Privacy Shield teilnehmenden Unternehmen (Datenimporteur) in den USA	Beitritt des US-Unternehmens zu dem Privacy Shield - Programm durch Beitrittserklärung, Registrierung auf einer Internet- Webseite und Veröffentlichung bestimmter Informationen; Datenexporteur muss in der EU seinen Sitz haben	Mitarbeiter-, Kunden-, Nichtkunden-, Interessenten- und Lieferantendaten im Rahmen der Registrierung	Keine Mitwirkung erforderlich; ggf. Hinweis des Übermittlers auf Teilnahme des Datenempfängers an dem Privacy Shield-Programm	Registrierung ab 01.08.2016 möglich.
Betriebsvereinbarung	Vereinbarung zwischen der Geschäftsleitung eines Unternehmens/Betriebs und dem Betriebsrat	Je nach Mandat des Betriebsrats variabel: zwischen einfachem Betrieb bis hin zu großen Konzerngebilden	Durch freiwillige Vereinbarung; hat den Rang einer Rechtsvorschrift i.S.d. § 4 Abs. 1 BDSG	I.d.R. nur Mitarbeiterdaten	Keine Mitwirkung erforderlich; ggf. Überprüfung bei einer Kontrolle durch die Aufsichtsbehörde	Setzt Betriebsrat voraus; die Reglungsreichweite einer Betriebsvereinbarung auf den Datentransfer in Drittländer ohne angemessenes Datenschutz-niveau wird zum Teil von Aufsichtsbehörden bezweifelt
Nichts tun	Keine Regelung implementieren	n.a.	n.a.	n.a.	n.a.	Hohes Risiko für die Verantwortlichen (Bußgeld/Haftstrafe) und das Unternehmen (Schadensersatz/Risiko der Untersagung der Geschäftstätigkeit/ des EDV-Betriebs/neg. Auswirkungen auf Image, Umsatz, Ertrag, Shareholder-Value)

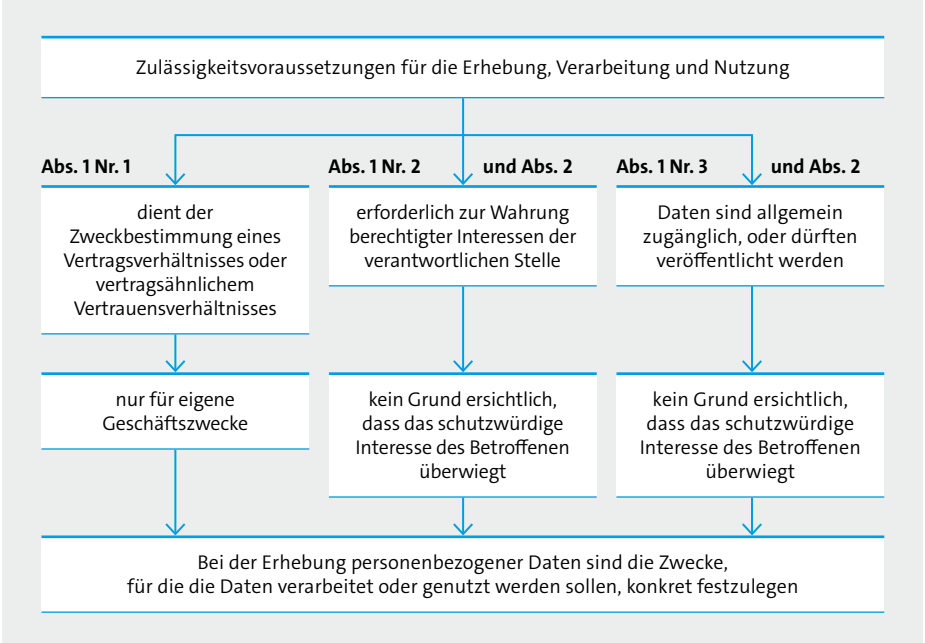
Quelle: AK Datenschutz und Datensicherheit der GSE Europe | Stand Juli 2004

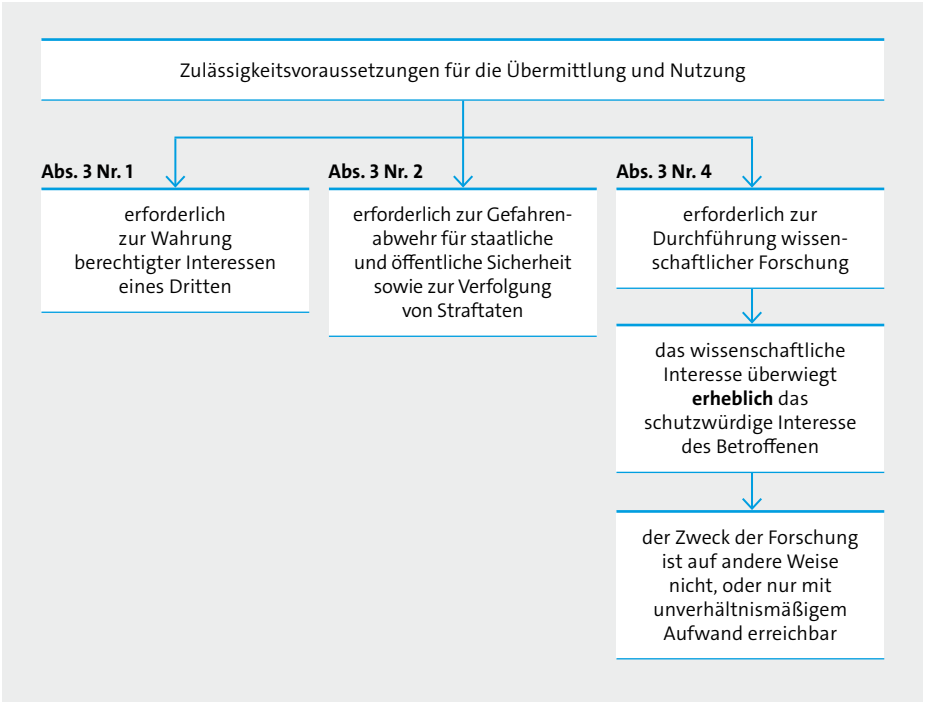
7.6 Möglichkeiten zur Erreichung eines angemessenen Datenschutzniveaus bzw. Ausnahmen vom Schutzerfordernis gem. §§4b, 4c Bundesatenschutzgesetz (BDSG)?



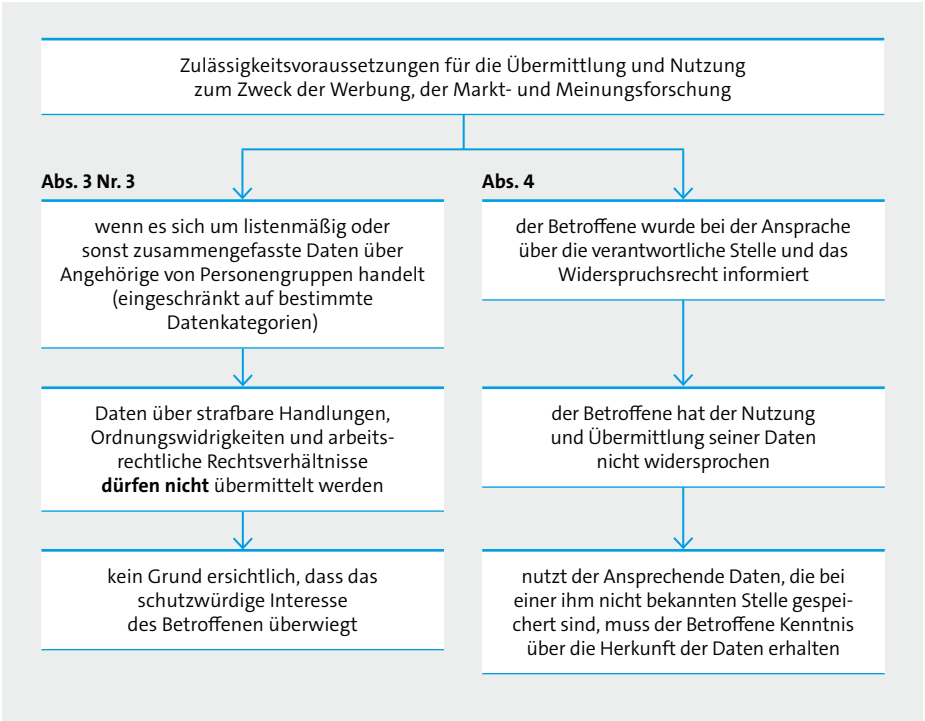
11 Übermittlung liegt auch vor, wenn der Datenempfänger Daten online abruft; bei Drittländern liegt außerdem auch bei der Datenverarbeitung im Auftrag eine Übermittlung vor.
12 Drittländer sind alle Staaten mit Ausnahme der EU-Staaten und der Staaten des Europäischen Wirtschaftsraumes (z. Zt. Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Großbritannien, Irland, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Österreich, Polen, Portugal, Schweden, Slowakei, Spanien, Tschechische Republik, Ungarn, Zypern sowie die EWR-Staaten Island, Liechtenstein und Norwegen).
13 Zur Zeit sind als Länder mit angemessenem Datenschutzniveau Argentinien, Guernsey, Isle of Man, Kanada und die Schweiz von der EU-Kommission anerkannt.
14 Programm für US-Unternehmen, die sich eindeutig und öffentlich verpflichtet haben, die sogenannten Privacy Shield Principles einzuhalten (s. ↗ Privacy Shield Liste).
15 Siehe die Entscheidungen ↗ hier.

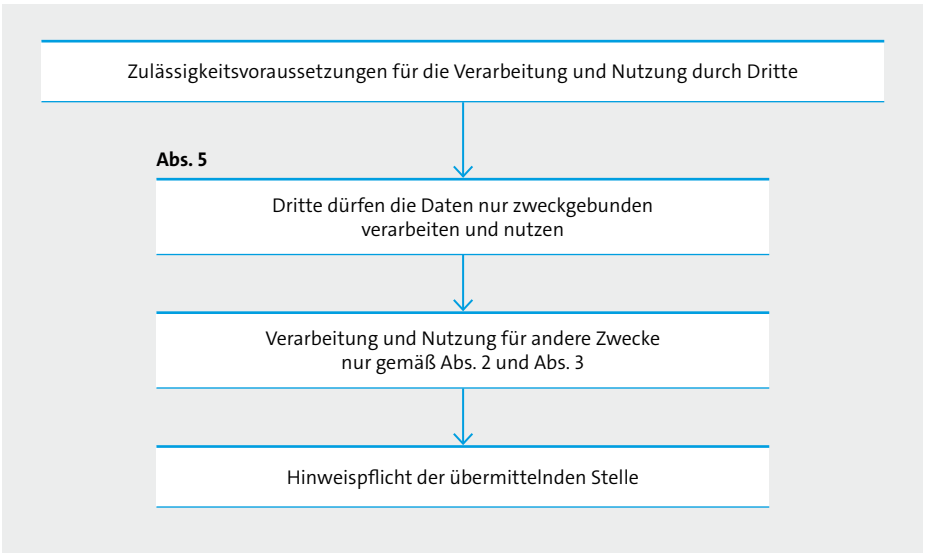
7.7 §28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke

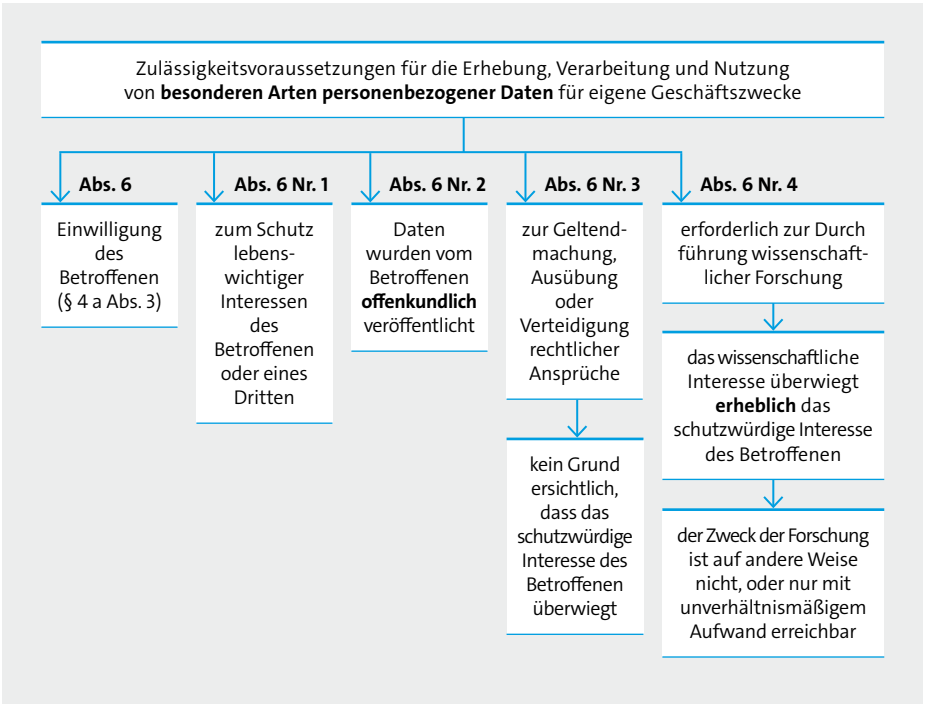


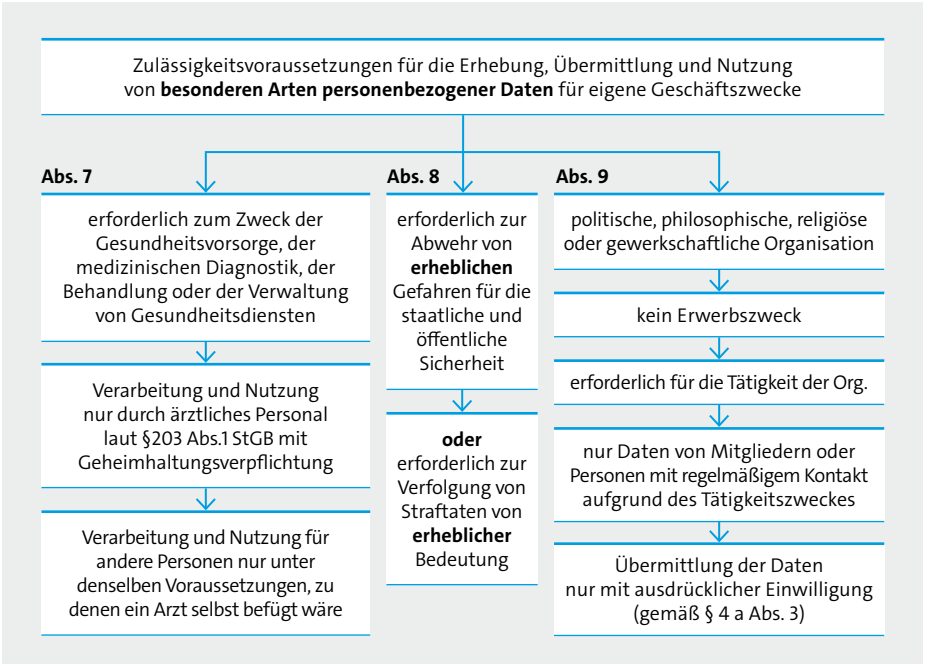


Grafik: Wolfgang Braun (Giesecke & Devrient), Ralf Maruhn (Nokia GmbH)


Zulässigkeitsvoraussetzungen für die Übermittlung und Nutzung zum Zweck der Werbung, der Markt- und Meinungsforschung
Abs. 3 Nr. 3
wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige von Personengruppen handelt (eingeschränkt auf bestimmte Datenkategorien)
Daten über strafbare Handlungen, Ordnungswidrigkeiten und arbeitsrechtliche Rechtsverhältnisse **dürfen nicht** übermittelt werden
kein Grund ersichtlich, dass das schutzwürdige Interesse des Betroffenen überwiegt
Abs. 4
der Betroffene wurde bei der Ansprache über die verantwortliche Stelle und das Widerspruchsrecht informiert
der Betroffene hat der Nutzung und Übermittlung seiner Daten nicht widersprochen
nutzt der Ansprechende Daten, die bei einer ihm nicht bekannten Stelle gespeichert sind, muss der Betroffene Kenntnis über die Herkunft der Daten erhalten


Zulässigkeitsvoraussetzungen für die Verarbeitung und Nutzung durch Dritte
Abs. 5
Dritte dürfen die Daten nur zweckgebunden verarbeiten und nutzen
Verarbeitung und Nutzung für andere Zwecke nur gemäß Abs. 2 und Abs. 3
Hinweispflicht der übermittelnden Stelle


Zulässigkeitsvoraussetzungen für die Erhebung, Verarbeitung und Nutzung von **besonderen Arten personenbezogener Daten** für eigene Geschäftszwecke
Abs. 6
Einwilligung des Betroffenen (§ 4 a Abs. 3)
Abs. 6 Nr. 1
zum Schutz lebens-wichtiger Interessen des Betroffenen oder eines Dritten
Abs. 6 Nr. 2
Daten wurden vom Betroffenen **offenkundlich** veröffentlicht
Abs. 6 Nr. 3
zur Geltend-machung, Ausübung oder Verteidigung rechtlicher Ansprüche
kein Grund ersichtlich, dass das schutzwürdige Interesse des Betroffenen überwiegt
Abs. 6 Nr. 4
erforderlich zur Durch führung wissenschaft-licher Forschung
das wissenschaftliche Interesse überwiegt **erheblich** das schutzwürdige Interesse des Betroffenen
der Zweck der Forschung ist auf andere Weise nicht, oder nur mit unverhältnismäßigem Aufwand erreichbar


Zulässigkeitsvoraussetzungen für die Erhebung, Übermittlung und Nutzung von **besonderen Arten personenbezogener Daten** für eigene Geschäftszwecke
Abs. 7
erforderlich zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Behandlung oder der Verwaltung von Gesundheitsdiensten
Verarbeitung und Nutzung nur durch ärztliches Personal laut §203 Abs.1 StGB mit Geheimhaltungsverpflichtung
Verarbeitung und Nutzung für andere Personen nur unter denselben Voraussetzungen, zu denen ein Arzt selbst befügt wäre
Abs. 8
erforderlich zur Abwehr von **erheblichen** Gefahren für die staatliche und öffentliche Sicherheit
oder
erforderlich zur Verfolgung von Straftaten von **erheblicher** Bedeutung
Abs. 9
politische, philosophische, religiöse oder gewerkschaftliche Organisation
kein Erwerbszweck
erforderlich für die Tätigkeit der Org.
nur Daten von Mitgliedern oder Personen mit regelmäßigem Kontakt aufgrund des Tätigkeitszweckes
Übermittlung der Daten nur mit ausdrücklicher Einwilligung (gemäß § 4 a Abs. 3)

8 Weiterführende Links und Literatur

8 Weiterführende Links und Literatur

↗ Arbeitspapiere der Art. 29 Datenschutzgruppe

↗ DLA Piper: Data Protection Laws of the Worlds

↗ Entschließungen des Düsseldorfer Kreises
(Oberste Datenschutzaufsichtsbeörden für den nicht-öffentlichen Bereich)

↗ International Conference of Data Protection & Privacy Commissioners

↗ Virtuelles Datenschutzbüro

V.Backes/H.Eul/M. Guthmann/R. Martwich/M. Schmidt in RDV 2004 S. 156:
»Entscheidungshilfe für die Übermittlung personenbezogener Daten in Drittländer«

Hinweis zum Datenschutz Nr. 39 des Innenministeriums Baden-Württemberg, Staatsanzeiger Baden-Württemberg Nr. 2 vom 24.01.2000 S. 12

Christoph Kuner / Jörg Hladjk in RDV 2005 S. 193 ff »Die alternativen Standardvertragklauseln der EU für internationale Datenübermittlungen«

Alexander Filip in ZD 2013 S. 51, 54
»Binding Corporate Rules (BCR) aus der Sicht einer Datenschutzaufsichtsbehörde«

Barbara Schmitz / Jonas von Dall´Armi in ZD 2016, S. 217 ff ,»Standardvertragsklauseln – heute und morgen – Eine Alternative für Datentransfer in Drittländer?«

Barbara Schmitz / Jonas von Dall'Armi in ZD 2016, S. 427 ff, »Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung?«

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 79 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, weitere 9 Prozent kommen aus Europa, 8 Prozent aus den USA. 4 Prozent stammen aus Asien, davon die meisten aus Japan. Bitkom fördert die digitale Transformation der deutschen Wirtschaft und setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org