Rechtsanwältin Nina Diercks
M.Litt (University of Aberdeen, Scotland)

Inhaberin der Anwaltskanzlei Diercks

https://diercks-digital-recht.de

Datenübermittlung im Konzern
Rechtsgrundlagen und formelle Anforderungen
Oder auch: Existiert ein Konzernprivileg und sind Intercompany-Verträge eine Lösung?

Abstract

Der nachfolgende Beitrag beschäftigt sich mit den Fragen der Datenübermittlung im Konzern. Beleuchtet werden die zur Verfügung stehenden Rechtsgrundlagen sowie die formellen Anforderungen an die Datenübermittlung.

Im Rahmen der Rechtsgrundlagen findet eine intensive Auseinandersetzung mit dem Konzernprivileg der DSGVO und dessen Reichweite, auch im Hinblick auf die Übermittlung von sensiblen Beschäftigtendaten, statt.

Im Rahmen der formellen Anforderungen an die Datenübermittlungen werden nicht nur die gesetzlichen Anforderungen an die verschiedenen gesetzlichen Formen der Datenübermittlungen (CtC, JCC, DPA) herausgearbeitet, sondern diese auch in den Bezug zur Praxis gesetzt. In diesem Zusammenhang wird der verbreitete Intercompany-Vertrag als Lösung für Datenübermittlungen im Konzern kritisch in Frage gestellt.

Zur Autorin

Nina Diercks, M.Litt (University of Aberdeen) ist seit 2010 als Rechtsanwältin tätig und führt die Anwaltskanzlei Diercks. Rechtsanwältin Diercks arbeitet ausschließlich in den Bereich des IT-| Datenschutz- und des angrenzenden Arbeitsrechts. Daneben veröffentlicht sie regelmäßig wissenschaftliche Fachbeiträge (jedenfalls soweit es ihre Zeit zulässt).

Des Weiteren führt Nina Diercks, ebenfalls seit 2010, den Blog Diercks Digital Recht und ist regelmäßig als Referentin, Interviewpartnerin und (Gast-)Autorin gefragt.

Rechtsanwältin Nina Diercks
M.Litt (University of Aberdeen, Scotland)

https://anwaltskanzlei-diercks.de
kontakt@anwaltskanzlei-diercks.de

Hamburg, 10. Mai 2020

Rechtsanwältin Nina Diercks
M.Litt (University of Aberdeen, Scotland)
Inhaberin der Anwaltskanzlei Diercks

DIERCKS DIGITAL RECHT
https://diercks-digital-recht.de

Inhaltsverzeichnis

Hamburg, 10. Mai 2020

1. Einleitung

Datenverarbeitungen in Konzernstrukturen sind vielschichtige Vorgänge gegenseitiger Übertragungsvorgänge und Abhängigkeiten. Die verschiedenen Konzernunternehmen verbindet ein Band vieler Ströme von personenbezogenen Daten wie es sich kaum zwischen anderen formal-juristisch unabhängigen juristischen Personen findet.

Ein typisches Praxisbeispiel sieht dabei aus wie folgt: Ein Konzern will die Personalverwaltungsaufgaben, die für jedes Unternehmen im Konzern recht gleichlaufend anfallen, zentralisieren und hierzu eine eigene juristische Person errichten – eine Personal GmbH –, die die zentralen Aufgaben der Personalverwaltung für alle Unternehmen im Konzernverbund übernimmt. Zu diesem Zweck übermitteln nun die Konzernunternehmen die personenbezogenen Daten ihrer Beschäftigten an die Personal GmbH. Die übermittelten Daten umfassen dabei etwa zur ordnungsgemäßen Berechnung der Steuern und Abgaben auch sensible Daten der Beschäftigten i.S.d. Art. 9 DSGVO, etwa die Religionszugehörigkeit und Gesundheitsdaten.

Derartige Formen der Konzernzentralisierung von Funktionsaufgaben wie Personal, IT oder Controlling, die auch als Shared Service Center bezeichnet werden sind nur eine von mehreren in der Praxis sehr häufig vorkommenden Konzernlösung bei der Daten sowohl horizontal als auch vertikal über verschiedene Konzernteile verarbeitet werden. Dennoch ist die Datenverarbeitung im Konzern nur am Rande von der DSGVO adressiert. Dies ist der Auslöser für mehrere Streitigkeiten, die in der Praxis von hoher Relevanz sind und mit diesem Aufsatz einer genaueren Betrachtung unterzogen werden.

Erörtert werden im Folgenden die Rechtsgrundlagen für eine Datenübermittlung insbesondere im Hinblick auf das „kleine“ Konzernprivileg einschließlich des Problems der Übermittlung auch sensibler Daten. Im Anschluss folgt eine Auseinandersetzung mit den formellen Anforderungen einer Datenübermittlung im Konzern inklusive der Frage, ob Intercompany-Verträge tatsächlich die Mutter aller Lösungen sind. Und schließlich wird noch ein Blick auf die Anforderungen an Datenübermittlungen in unsichere Drittstaaten geworfen.

2. Datenübermittlung im Konzern

Bekanntermaßen bedarf jede Datenverarbeitung und so auch die stets einer Rechtsgrundlage im Sinne von Art. 6 DSGVO.[1]

Daneben besteht bei einer Datenübermittlung im Konzern die Frage, ob aufgrund der Art des Verhältnisses der übermittelnden Parteien seitens der DSGVO zusätzliche Maßnahmen zum Schutz der personenbezogenen Daten bzw. der Betroffenen ergriffen und formelle Anforderungen erfüllt werden müssen.

So sieht die DSGVO grundsätzlich bei einer Auftragsverarbeitung nach Art. 28 DSGVO sowie bei einer Verarbeitung von Daten in gemeinsamer Verantwortung nach Art. 26 DSGVO vor, dass die Parteien diesbezügliche Vereinbarungen treffen.

[1] *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 2019, Art. 5 R. 5.

3. Rechtsgrundlagen der Datenübermittlung im Konzern

Die Datenübermittlung zwischen zwei juristischen Personen bedarf einer Rechtsgrundlage im Sinne von Art. 6 DSGVO. Dies gilt auch im Grundsatz für juristische Personen, die im Rahmen eines Konzerns miteinander verbunden sind.

Bei der Betrachtung von möglichen Rechtsgrundlagen für eine Datenübermittlung im Konzern muss jedoch zunächst eine Auseinandersetzung zur Frage des Konzernprivilegs der DSGVO erfolgen.

3.1. Das „kleine" Konzernprivileg der DSGVO

Vor der DSGVO galt der Satz: „Kein Konzernprivileg im Datenschutz!". Dies bedeutete, dass jede Tochter eines Konzerns schlicht als „Dritter" betrachtet und die Datenübermittlung rechtlich abgesichert werden musste. Das führte in der Theorie zu großen Problemen, da zwar die EU-Datenschutz-Richtlinie schon das Konstrukt der gemeinsamen Verantwortung und damit solcher Vertragskonstellationen kannte, das BDSG jedoch nur den Auftragsdatenverarbeitungsvertrag. Das hatte zur Folge, dass faktisch jede konzernweite Datenverarbeitung als Auftragsdatenverarbeitung im Sinne von § 11 BDSG qualifiziert wurde, wenn man nicht mit dem Konstrukt der „Funktionsübertragung" die Gestaltung von Auftragsdatenverarbeitungsverträgen vermeiden konnte. Da dies jedoch Rechtshistorie ist und sich auch praktisch nur die wenigstens Konzerne vor der DSGVO mit ordnungsgemäßen Datenübermittlungen auseinandersetzten, lasse ich es hierbei bewenden.

Im Gesetzestext der DSGVO wurde, obwohl dies im Gesetzgebungsverfahren zur Diskussion stand,[2] im Ergebnis ebenfalls keine besondere Rechtsgrundlage zur Datenverarbeitung und vor allem der Datenübermittlung im Konzernverbund aufgenommen. Insoweit existiert weiterhin keine Konzernprivilegierung im engeren Sinne. Demnach ist zunächst weiter jeder Unternehmensteil als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO zu betrachten, so dass die Übermittlung von personenbezogenen Daten an einen anderen Konzernteil zunächst wie eine Datenübermittlung an Dritte betrachtet werden muss.[3]

Dennoch hat die DSGVO die Datenübermittlung im Konzern nicht unbeachtet gelassen.

Zunächst findet sich in Art. 4 Nr. 19 DSGVO die Definition der Unternehmensgruppe. Es handelt sich um *eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht.*

Zur Unternehmensgruppe werden in den Erwägungsgründen, also den Interpretationshilfen des Gesetzgebers, verschiedentlich Ausführungen gemacht:

In Erwägungsgrund 37 heißt es: „*Eine Unternehmensgruppe sollte aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen bestehen, wobei das herrschende Unternehmen dasjenige sein sollte, das zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann. Ein Unternehmen, das die*

[2] Simitis/Hornung/Spiecker gen. Döhmann – Schantz, Datenschutzrecht, 1. Auflage 2019, Art. 6, Rn. 116.
[3] Vgl. Simitis/Hornung/Spiecker gen. Döhmann - Seifert, Datenschutzrecht, 1. Auflage 2019, Art. 88, Rn. 176; Kühling/Buchner – Maschmann, DS-GVO BDSG, 2. Auflage 2018, Art. 88, Rn. 52.

Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, sollte zusammen mit diesen als eine „Unternehmensgruppe" betrachtet werden."

Demnach ist ein Konzern eine als wirtschaftliche und rechtliche Einheit geführte Unternehmensgruppe unter einheitlicher Leitung zu verstehen, wobei wesentliches Merkmal einer Konzernstruktur das Bestehen eines wirtschaftlichen Beteiligungs- und Beherrschungsverhältnisses an grundsätzlich eigenständigen Unternehmen ist.[4]

In Erwägungsgrund 48 wird erläutert, in welchen Fällen eine Übermittlung von Daten innerhalb einer solchen Unternehmensgruppe zulässig ist: *Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.*

Der Gesetzgeber hat also die Notwendigkeit einer Privilegierung gesehen und insoweit die berechtigten Interessen an der Datenübermittlung im Rahmen von Unternehmensgruppen über EG 48 in Art. 6 I f) DSGVO hervorgehoben, so dass dem Verantwortlichen die Möglichkeit gegeben ist, sich bei einer Datenübermittlung im Konzern in den vorgenannten Fällen auf die berechtigten Interessen berufen zu können.[5]

Dabei ist die häufig anzutreffende Lesart, es handele sich um keine „echte Privilegierung", da eine solche im Gesetzestext und nicht in den Erwägungsgründen zu finden sein müsse, so nicht richtig. Richtig ist zwar, dass sich in dem Gesetzestext der DSGVO kein allgemeiner „Konzern"-Erlaubnistatbestand, der jegliche Übermittlungen im Konzernkontext erlaubt, zu finden ist. Eine solche Klausel, die unbedingt Übermittlungen im Konzern erlaubt, wäre aber auch zu weitgehend und hätte die Interessen der Betroffenen (Kunden, Beschäftigte) nicht hinreichend berücksichtigt. Folglich hätte ein „Konzern"-Erlaubnistatbestand ebenfalls eine Angemessenheits- und Abwägungsklausel enthalten müssen, um zu einem solchen Ausgleich zu gelangen. Eine solche „Konzernklausel" wäre aber wiederum redundant gewesen, da mit Art. 6 I f) DSGVO bereits eine eben solche Interessensabwägungsklausel existiert. Insoweit war es nur notwendig, über den Erwägungsgrund 48 klarzustellen, dass Konzerne ein berechtigtes Interesse an Datenübermittlungen von Kunden und Beschäftigtendaten zu internen Verwaltungszwecken haben können. Damit wird die Übermittlung von Daten im Konzern insoweit im Rahmen der berechtigten Interessen dadurch privilegiert, dass Konzerne für eine Datenübermittlung „nur" eine Interessensabwägung vornehmen müssen, bei der der Gesetzgeber grundsätzlich davon ausgeht, dass eben berechtigte Interessen seitens des Konzerns vorliegen können.

[4] Vgl. Bussche v.d./Voigt, Konzerndatenschutz, 2. Auflage 2019, Kap.1, Rn. 1.
[5] Unter vielen: Gola – Schulz, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 6, Rn. 104 u 195; Kühling/Buchner – Buchner/Maschmann, DSGVO BDSG, 2. Auflage 2018, Art. 6 Rn. 168 und Art. 88, Rn. 73; Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil VI, Kapitel 1, Rn. 15 f.; Pfrang - PinG, 04/19, 163; Voigt, Praxisanleitung zur Schaffung eines Konzernprivilegs, CR 2017, 429.

3.2. Artikel 6 DSGVO und das „kleine" Konzernprivileg

Die Rechtsgrundlage zur Datenübermittlung in Form von Art. 6 I f) DSGVO iVm EG 48 wird deswegen auch als das „kleine Konzernprivileg" bezeichnet.[6] Dabei kann diese Bezeichnung aus den vorgenannten Gründen kritisch gesehen werden. Schließlich handelt es sich faktisch um keine „kleine" Privilegierung, sondern um eine schlichte Privilegierung von bestimmten Konzernübermittlungen.

Je nach Verarbeitungssituation können neben Art. 6 I f) in Verbindung mit EG 48 noch weitere mögliche Rechtsgrundlagen zur Übermittlung existieren wie:

- Art. 6 I b) iVm Art. 88 DSGVO, § 26 I BDSG – bei Beschäftigtendaten soweit nach dem Arbeitsverhältnis erforderlich (im Ergebnis aber gleiche Abwägung wie bei Art. 6 I f) DSGVO)
- Art. 6 I b) iVm Art. 88 DSGVO, § 26 I BDSG – Arbeitsvertragliche Klauseln im Hinblick auf Beschäftigtendaten (insb. bei Matrix-Strukturen)
- Art. 88 DSGVO, § 26 I BDSG – Kollektivvereinbarungen, Betriebsvereinbarungen hin. Beschäftigtendaten (diese können Datenübermittlungen jedoch nur konkretisieren, nicht aber über die Rechtsgrundlagen der DSGVO hinausgehen)
- Corporate Binding Rules, Art. 47 DSGVO, angelegt an sich für/bei Drittstaatenübermittlung
- Art. 6 I a) Einwilligung.

Diese Ermächtigungsgrundlagen jeweils dezidiert zu betrachten, würde den Umfang der Erörterung sprengen, demnach findet nachfolgend maßgeblich eine Konzentration auf Art. 6 I f) DSGVO in Verbindung mit Erwägungsgrund 48 statt. Daneben wird zuweilen am Rande auch Art. 6 I b) iVm EG 48 betrachtet werden.

3.2.1. Auswirkungen auf die Interessensabwägung und die Erforderlichkeitsprüfung

Nach Art. 6 I f) DSGVO ist die Datenverarbeitung – wozu auch die Übermittlung zählt – zulässig, *wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen*.

Mit Erwägungsgrund 48 erkennt der Unionsgesetzgeber an, dass innerhalb von Unternehmensgruppen ein *gesteigertes Bedürfnis* nach Datenübermittlungen für *interne Verwaltungszwecke,* einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, besteht.[7] Es wird demnach abstrakt das „berechtigte Interesse" der verbundenen Unternehmen an Datenübermittlungen im Sinne des Abwägungsmodells des Art. Art. 6 I f) DSGVO anerkannt.[8]

Das entbindet den Konzern bzw. den jeweiligen Konzernteil natürlich nicht davon, die Interessensabwägung hinsichtlich der vorliegenden Datenverarbeitung nach Art. 6 I f) DSGVO oder die

[6] So auch: Bussche v.d./Voigt, Konzerndatenschutz, 2. Auflage 2019, Kap.1, Rn. 7; Voigt, Praxisanleitung zur Schaffung eines Konzernprivilegs, CR 2017, 429.
[7] Bussche v.d./Voigt, Konzerndatenschutz, 2. Auflage 2019, Teil 3, Kap. 1, Rn. 7; BeckOK Datenschutzrecht, Wolff/Brink - Albers/Veit, 28. Edition, Art. 6, Rn. 49.
[8] Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil 6, Kapitel 1, Rn. 16.

nach Art. 6 I b), Art. 88 DSGVO iVm. § 26 BDSG (im Rahmen der Erforderlichkeitsprüfung) auch vorzunehmen.

Bei dieser konkreten Interessensabwägung ist jedoch zum einen die Privilegierung aus EG 48 zu beachten. Aus dieser folgt, dass bei einer konzerninternen Übermittlung die berechtigten Interessen der Unternehmen in der Regel höher und die schutzwürdigen Interessen der betroffenen Personen niedriger zu bewerten sind als beim Datentransfer zwischen konzernfremden Unternehmen.[9] Zum anderen ist bei der Interessensabwägung stets zu berücksichtigen, ob die betroffene Person mit der Verarbeitung der Daten durch andere Konzernunternehmen rechnen musste.[10]

Letzteres ist in der Regel der Fall. Regelmäßig ist den Mitarbeitern die Konzernstruktur bekannt und bewusst, dass in Konzernstrukturen andere Unternehmensteile für spezielle Geschäftsbereiche und deren Datenverarbeitungen verantwortlich sind, also, dass etwa die Personaldaten in einer Personal GmbH des Konzerns verarbeitet werden. Jedenfalls müssen Mitarbeiter im Rahmen der Information zur Datenverarbeitung gemäß Art. 12, 13 DSGVO über die Datenverarbeitung und folglich auch über die Empfänger der Daten aufgeklärt werden. Gleiches gilt im Ergebnis für Kundendaten, so etwa, wenn die Kundendaten in einer zentralen CRM-Datei verwaltet werden. [11]

Regelmäßig wird im Ergebnis das Interesse der betroffenen Person hinter das berechtigte Interesse des Unternehmens an der Datenübermittlung zurücktreten, weil die Datenübertragung entweder ohnehin erforderlich im Sinne der Art. 6 I b), 88 DSGVO iVm § 26 BDSG ist oder aber der Datenübertragung jedenfalls keine Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person im Sinne des Art. 6 I f) DSGVO überwiegend entgegenstehen werden.

3.2.2. Zwischenfazit zu Art. 6 DSGVO und dem „kleinen" Konzernprivileg

Insgesamt wird bei der Übermittlung von Kunden- oder Beschäftigtendaten innerhalb des Konzernverbundes regelmäßig das Vorliegen eines berechtigten Interesses in diesem Sinne zu begründen sein, auch da die Gewichtung des Gesetzgebers mit Erwägungsgrund 48 eben in der Abwägung zu berücksichtigen ist.[12]

Diese bis mit dem (kleinen) Konzernprivileg zu einem gewissen Grad prädisponierte Wertung des Gesetzgebers bezüglich der Datenübermittlung im Konzern ist praxisnotwendig. Ein solcher Datenaustausch gehört schließlich zum unabdingbaren Tagesgeschäft.[13]

3.3. Die Übermittlung von sensiblen Beschäftigtendaten im Konzern

Streitig ist aber, ob die Privilegierung des Erwägungsgrund 48 dann genügt, wenn sensible Daten Gegenstand der Übermittlung sind.

---

[9] *Plath* in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 6 DSGVO, Rn. 77
[10] Simitis/Hornung/Spiecker gen. Döhmann – Schantz, Datenschutzrecht, 1. Auflage 2019, Art. 6, Rn. 116.
[11] Vgl. *Plath* in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 6 DSGVO, Rn. 77
[12] Unter vielen: Gola – Schulz, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 6, Rn. 104 u 195; Kühling/Buchner – Buchner/Maschmann, DSGVO BDSG, 2. Auflage 2018, Art. 6 Rn. 168 und Art. 88, Rn. 73; Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil VI, Kapitel 1, Rn. 15 f.; Pfrang - PinG, 04/19, 163; Voigt, Praxisanleitung zur Schaffung eines Konzernprivilegs, CR 2017, 429.
[13] Ehmann/Selmayr - Selk, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 88, Rn. 172..;

Insbesondere in der Personalverwaltung müssen aber sensible Daten übermittelt werden. Schließlich können etwa Steuern und Sozialabgaben nur dann regelgerecht abgeführt werden, wenn die Religionszugehörigkeit bekannt ist. Gesundheitsdaten sind hingegen unter anderem bei der Durchführung eines beruflichen Eingliederungsmanagements (BEM) notwendig.

Als Rechtsgrundlage für die Übermittlung kommt in diesen Fällen Art. 6 I b), Art. 9 II b), Art. 88 DSGVO iVm § 26 BDSG iVm EG 48 in Betracht.[14]

3.3.1. Erforderlichkeit einer Übermittlung sensibler Beschäftigtendaten

Die Verarbeitung personenbezogener sensibler Daten ist im Grundsatz ein Eingriff von besonders schwerem Gewicht. Die Verarbeitung ist grundsätzlich verboten. Aus diesem Umstand ließe sich schließen, dass eine Übermittlung an Dritte zur Erfüllung des Arbeitsverhältnisses nicht mehr erforderlich sein kann[15] und sensible Daten stets durch den Arbeitgeber selbst zu verarbeiten wären.

§ 26 III BDSG erlaubt jedoch gerade die Verarbeitung von sensiblen Daten iSd Art. 9 I DSGVO, wenn sie erforderlich ist, *damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedsstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedsstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist.* Damit setzt § 26 III BDSG den Erlaubnistatbestand von Art. 6, Art. 9 II b) DSGVO um.[16] Diese Erlaubnis zur Verarbeitung sensibler Daten gilt aufgrund seiner systematischen Stellung als eigener Absatz sowohl für Verarbeitungen, die auf Grundlage der Einwilligung der betroffenen Person erfolgen (§ 26 II BDSG), als auch für Verarbeitungen, die im Rahmen der Vertragserfüllung erforderlich sind (§ 26 I BDSG).

Ist die Verarbeitung sensibler Daten demnach gestattet, ist gemäß § 26 III 3 BDSG der § 22 II BDSG entsprechend anzuwenden. Danach müssen *spezifische Verfahrensregelungen [bestehen], die im Fall einer Übermittlung […] die Einhaltung der Vorgaben dieses Gesetzes sowie der [DSGVO] sicherstellen*.

Übermittlungen sensibler Daten im Beschäftigungsverhältnis müssen also spezifischen Verfahrensregelungen unterliegen. Daraus folgt, dass eine Übermittlung im Grundsatz zulässig ist. Ansonsten wäre die gesetzliche Anordnung des Erfordernisses spezifischer Verfahrensregeln für sensible Daten sinn- und zwecklos.

Folglich muss auch die Übermittlung sensibler Daten im Grundsatz unter § 26 I BDSG möglich sein, sonst würde der Verweis in § 26 III 3 BDSG ins Leere laufen. Natürlich befreit dies das Unternehmen nicht von der Prüfung, ob die Übermittlung an Dritte zur Erfüllung des Arbeitsverhältnisses auch tatsächlich „erforderlich“ ist.

---

[14] Die Verfasserin sieht in Art. 9 keine eigenständigen Rechtsgrundlagen, sondern ausschließlich Vorgaben des Gesetzgebers zur Verarbeitung von sensiblen Daten, die neben den Voraussetzungen der Rechtsgrundlagen von Art. 6 im Fall des Vorliegens sensibler Daten beachtet werden müssen.

[15] So auch: *Riesenhuber*, in: BeckOK DatenschutzR Wolff/Brink, 28. Ed. 2019, § 26 R. 183.

[16] *Gräber/Nolden*, in: Paal/Pauly, 2. Aufl. 2018, § 26 R. 41.

Mit der Feststellung, dass eine Eigenverarbeitungspflicht systematisch nach §§ 26 III 3 iVm 22 II Nr. 10 BDSG nicht bestehen kann, ist bei der Beantwortung der Frage, ob sensible Daten an ein SSC übermittelt werden dürfen, anhand des Gesetzes und damit anhand der Erforderlichkeit zu bewerten.

3.3.2. Interessensabwägung bei der Übermittlung von sensiblen Beschäftigtendaten

Maßgeblich ist damit, ob die Verarbeitung in Form der Übermittlung erforderlich iSd. § 26 III BDSG iVm. Art. 9 II b) DSGVO ist. Das heißt im Ergebnis nichts anderes, als zu prüfen, ob der Arbeitgeber berechtigte Interessen vorweisen kann und schutzwürdigen Interessen der betroffenen Person nicht überwiegen.

Dabei ist zu beachten, dass dem Arbeitgeber zunächst einmal die unternehmerische Freiheit zusteht, zu entscheiden, wie er seinen Betrieb organisiert; es ist nicht Sache der Gerichte oder Behörden, über Betriebsabläufe und ihre Organisation zu entscheiden, und der Arbeitgeber ist bei der Organisation nicht gebunden, den Weg zu wählen, auf dem die wenigsten Datenverarbeitungen anfallen.[17] Das entbindet den Verantwortlichen natürlich nicht von der Vornahme der weiteren Interessensabwägung. Im Hinblick auf die Übermittlung von sensiblen Daten ist jedoch im Hinblick auf das Interesse der betroffenen Arbeitnehmer das Folgende zu beachten.

3.3.2.1. Vorhersehbarkeit der Übermittlung

Dem Arbeitnehmer ist regelmäßig die konzerninterne Struktur und die Abrechnungs- und Verwaltungssystematik bekannt, eine diesbezügliche Übermittlung personenbezogener Daten ist für ihn „vorhersehbar“. Spätestens mit den zwingenden Informationen zur Datenverarbeitung nach Art. 12, 13 DSGVO wird der Arbeitnehmer hierrüber in Kenntnis gesetzt.

Im Rahmen dieser vorhersehbaren Übermittlung muss der Arbeitnehmer auch mit Übermittlung sensibler Daten rechnen. Ihm ist bekannt, dass der Arbeitgeber personenbezogene Daten iSd. Art. 9 I DSGVO benötigt, um den Betrieb ordnungsgemäß zu führen und seinen Pflichten etwa gegenüber den Sozialversicherungen nachzukommen.

Die Annahme, personenbezogene Daten würden zum Zwecke der Personalverwaltung übermittelt ohne dass dabei auch sensible Daten übermittelt würden, muss dem Arbeitnehmer als lebensfremd vorkommen. Hieraus folgt, dass ein schutzwürdiges Interesse des Betroffenen jedenfalls nicht schematisch überwiegen muss.[18]

Das Kriterium der Vorhersehbarkeit muss sich demnach auf alle Arten sensibler Daten beziehen.

3.3.2.2. Geringe Gefahr durch gesetzlichen Schutz

Maßgeblich für das schutzwürdige Interesse des Arbeitnehmers ist insbesondere, ob ein hoher Schutz seiner personenbezogenen, sensiblen Daten gewährleistet ist.

Gerne wird hier argumentiert, dass die Gefahr bestünde, durch die Übermittlung der Daten an eine anderweitige Konzerntochter, die das SSC stellt, würde eine unkontrollierbare Verarbeitung entstehen können. Ob bei einer Übertragung an ein SSC das Schutzniveau tatsächlich abgesenkt wird, ist deshalb diskussionswürdig.

---

[17] BeckOK DatenschutzR/Riesenhuber, BDSG, § 26, Rn. 114, mwN.
[18] Erw.-Gr. 47 S. 4; LINK.

Zum einen ist ein SSC ist in der Regel als juristisch selbstständige Person ausgestaltet, zum Beispiel als eigenständige GmbH. Herrschenden Einfluss besitzt in der GmbH die Gesellschafterversammlung, die über den Gesellschaftsvertrag bzw. § 46 Nr. 6 GmbHG den Geschäftsbetrieb überwachen können. Regelmäßig hält die Konzernmutter einen nicht unerheblichen Anteil. Damit gewinnt die Konzernmutter einen rechtlich abgesicherten Einfluss auf das SSC und kann verbindlich anweisen, dass die sensiblen Daten des Arbeitnehmers auch tatsächlich nur zur Personalverwaltung verwendet werden. Die Gefahr, dass durch eine divers besetzte Gesellschafterversammlung mit völlig unbeteiligten Dritten durch Beschlüsse andere Weisungen erlassen werden, ist so praktisch nicht ersichtlich.

Zum anderen – und das ist noch wesentlich wichtiger – ist der Schutz der zweckgebundenen Datenverarbeitung schon durch die DSGVO selbst gewährleistet, nämlich durch Art. 6 IV DSGVO. Eine Abänderung des Zwecks „Personalverwaltung“ wäre in der Regel ein sanktionierbarer Datenschutzverstoß des SSC (etwa der „Personal GmbH“).

3.3.2.3. Wertung des „kleinen“ Konzernprivilegs bei sensiblen Beschäftigtendaten

Wie oben schon festgestellt, besteht an der konzerninternen Übermittlung von personenbezogenen Daten regelmäßig ein berechtigtes Interesse des Verantwortlichen, welches sich in Erwägungsgrund 48 begründet.

Nun könnte dieses berechtigte Interesse im Rahmen des § 26 III BDSG iVm. Art. 9 II b) DSGVO nicht mehr ausreichend sein, um auf Seiten des verantwortlichen Arbeitgebers für ein Übermittlungsrecht an ein SSC zu streiten.

Eine solche Beschränkung ist im Wortlaut des Erwägungsgrunds 48 nicht ersichtlich, dieser scheint auf eine Festlegung berechtigter Interessen verordnungsübergreifend angelegt.

Teleologisch jedoch könnte die Annahme zu treffen sein, dass ein Erwägungsgrund nicht ausreichen kann, ein Regel-Ausnahme-Verhältnis im Gesetzeswortlaut im engeren Sinne umzukehren. Diese teleologische Erwägung ist allerdings aus zwei Gründen nicht maßgebend: Zum einem darf nicht verkannt werden, dass auch Erwägungsgründe Teil des Gesetzes sind. Zum anderen ging der Gesetzgeber davon aus, dass es keine Grundannahme geben darf, wonach die schutzwürdigen Interessen des Betroffenen grundlegend überwiegen.[19] Allein eine offene Prüfung der Verhältnismäßigkeit ist maßgeblich.[20]

Wenn eine solche Grundannahme gar nicht überwunden werden muss, dann kann sie schon gar nicht so schwer wiegen, als dass zu ihrer Überwindung ein schlichter Erwägungsgrund nicht ausreiche.

Auf einen zweiten Blick wäre die Ausklammerung von sensiblen Daten aus Erwägungsgrund 48, mithin die Nichtprivilegierung, schon widersinnig. Denn ausweislich des Wortlauts soll gerade für interne Verwaltungszwecke einschließlich der Verarbeitung von Beschäftigtendaten ein berechtigtes Interesse bestehen. Erwägungsgrund 48 liefe diesbezüglich wohl leer, wenn für interne Verwaltungszwecke zwar Beschäftigtendaten übermittelt werden dürfen, aber dann nicht, wenn sie sensible Daten enthalten. Eine Übermittlung zu internen Verwaltungszwecken wäre redundant.

[19] BT-Drucksache 18/11325, 98; LINK.
[20] BT-Drucksache 18/11325, 98; LINK.

Zusammenfassend ist weder Erwägungsgrund 48 mit einer Einschränkung versehen, noch ließe sich eine solche teleologisch befürworten, ohne den Anwendungsbereich faktisch leerlaufen zu lassen.

Erwägungsgrund 48 ist folglich auch bei der Übermittlung sensibler Daten an SSC geeignet, ein berechtigtes Interesse zu indizieren.

3.3.2.4. Zwischenfazit zur Übermittlung von sensiblen Beschäftigtendaten

Nach der Begründung des Gesetzgebers ist im Rahmen des § 26 III BDSG eine ergebnisoffene Abwägung vorzunehmen.

Auf Seiten des Arbeitgebers streitet für sein Recht, sensible Daten an ein SSC zu übermitteln, ein berechtigtes Interesse, seine Verwaltungsprozesse effizient zu bündeln und zentrale Dienstleistungen auszulagern, welches auch in Erwägungsgrund 48 seinen Niederschlag findet.

Ferner kann er durch seine gesellschaftsrechtlichen Einwirkungsrechte auch sicherstellen, dass die Missbrauchsgefahr minimiert wird und das SSC die personenbezogenen sensiblen Daten nur für den aufgegebenen Zweck verarbeitet. Dies wird flankiert durch sanktionierte Zweckänderungsverbote auf Seiten des SSC selbst. Korrespondierend hierzu senkt sich das schutzwürdige Interesse der betroffenen Person ab.

Der betroffene Arbeitnehmer musste vernunftgemäß damit rechnen und wurde darüber informiert, dass seine personenbezogenen Daten zwecks Personalverwaltung an das SSC übermittelt wurden. Dass dies nicht sensible Daten umfassen würde, wäre eine lebensfremde nicht schutzwürdige Annahme.

Schutzwürdige Interessen des Arbeitnehmers, die den vorigen Abwägungsgründen entgegenstehen, sind nicht in der Stärke erkennbar, als dass sie das berechtigte Interesse des Arbeitgebers überwögen.

Demnach kann eine Übermittlung von sensiblen Daten an ein SSC soweit auch erforderlich iSd. § 26 III BDSG sein.

3.3.3. Problem der Zweckbeschränkung des § 26 III BDSG

§ 26 III BDSG beschränkt allerdings Übermittlungszwecke bei der Übermittlung sensibler Daten. Nicht jeder im Rahmen einer Verarbeitung „erforderliche" Zweck reicht zur Legitimierung aus. Denn nach § 26 III BDSG ist die Datenverarbeitung nur *zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes* erforderlich. Relevant wird dies im Falle von SSC dort, wo Daten zwar zur Durchführung eines Beschäftigungsverhältnisses übertragen werden, ohne jedoch, dass diese sämtlich oder direkt einer gesetzlichen oder kollektivrechtlichen[21] Pflichterfüllung des Arbeitgebers dienen.

Nun meint eine Meinungsgruppe in der Literatur, dass unter § 26 III BDSG nur solche Verarbeitungen sensibler Daten im Arbeitsverhältnis legitimiert sind, die sich aus dem Gesetz selbst oder aus Kollektivvereinbarungen ergeben. Folge hieraus wäre, dass für alle anderen Formen der Verarbeitung sensibler Daten entweder eine andere Grundlage in Art. 9 II DSGVO gefunden werden muss oder der Arbeitgeber sich eine Einwilligung einholen muss.[22]

[21] *Kempert*, in: Sydow, 2. Aufl. 2018, Art. 9 R. 16; LINK.
[22] Verweisend: *Gola*, in: Gola/Heckmann, 13. Aufl. 2019, § 26 R. 145 f.; LINK.

Die vorzugswürdige Gegenauffassung hingegen lässt jede rechtliche Pflicht ausreichen, um sensible Daten im Beschäftigungsverhältnis zu verarbeiten. Als solche rechtliche Pflicht kommen vor allem auch der Arbeitsvertrag und seine Verpflichtungen in Betracht.[23] Hiernach wäre also auch die Verarbeitungen zur Erfüllung nicht primär gesetzlicher Pflichten über § 26 III BDSG möglich, sofern sie einen Bezug zum Arbeitsvertrag aufweist.

Dass letztgenannte Ansicht überzeugt, zeigt sich unter anderem an der gesetzgeberischen Begründung des § 26 III BDSG. Denn dort wird als Beispiel die Verarbeitung zur Feststellung der Arbeitsfähigkeit im Generellen als der Norm unterfallend genannt.[24]

Damit sind der Einsatz eines SSC zu allen Aufgaben im Rahmen der Personalverwaltung und die dafür notwendigen Datenübermittlungen möglich. Dies entspricht auch der Praxis.

Der Zweck einer umfassenden Personalverwaltung ist folglich auch ein tauglicher Zweck iSd. § 26 III BDSG bei der Übermittlung von personenbezogenen Daten an ein SSC.

3.3.4. Fazit zur Übermittlung sensibler Beschäftigtendaten

Damit ist zu konstatieren, dass auch die Übermittlung von sensiblen personenbezogenen Daten auf Grundlage von Art. 6 I b), Art. 9 II, Art. 88 DSGVO, § 26 BDGS iVm EG 48 grundsätzlich zulässig sein kann.

3.4. Rechtsgrundlage der Verarbeitung (sensibler) Daten für den empfangenden Konzernteil

Wurde im vorhergehenden Teil festgestellt, das an der Übermittlung von personenbezogenen Daten ein berechtigtes Interesse hat, so rechtfertigt dies noch nicht die Verarbeitung durch das empfangende Unternehmen.

Das empfangende Unternehmen muss die eigene Verarbeitungstätigkeit selbst auf eine taugliche Rechtsgrundlage stützen können.

Als Rechtsgrundlage kommt zum einen Art. 6 I b) ggf. iVm 9 II b) DSGVO in Betracht. Der empfangende Konzernteil ist regelmäßig vertraglich gegenüber dem anderen Konzernteil verpflichtet, die Datenverarbeitung (etwa Personalsachbearbeitung) vorzunehmen. In Folge dessen kann sich der empfangende Konzernteil auf diese vertragliche Grundlage stützen, die Datenverarbeitung ist zur Vertragsdurchführung notwendig.

Im Übrigen stritte auch Erwägungsgrund 48, die „kleine“ Konzernprivilegierung, in dem Fall, in dem man Art. 6 I f) DSGVO als Rechtsgrundlage begreifen wollen würde, auch zugunsten des SSC. Begriffsnotwendig ist bei Datenverarbeitungen in Konzernstrukturen nicht nur das aussendende, sondern auch das empfangende Unternehmen als privilegiert zu begreifen. Folglich wäre hier wiederum eine Interessensabwägung vorzunehmen. Hierbei kann auf die vorgenannten tragenden Erwägungen im verwiesen werden.

Die Verarbeitung personenbezogener Daten durch das SSC wird aber regelmäßig auf Art. 6 I b), 9 II b) DSGVO zu stützen sein.

---

[23] Verweisend: *Gola*, in: Gola/Heckmann, 13. Aufl. 2019, § 26 R. 147.; LINK.
[24] BT-Drucksache 18/11325, S. 98; LINK; Gola, in: Gola/Heckmann, 13. Aufl. 2019, § 26 Rn. 149; LINK.

4. Formelle Anforderungen an die Datenübermittlung im Konzern

Mit der Feststellung, dass mit Art 6 I f) bzw. Art. 6 I b) DSGVO iVm mit EG 48 grundsätzlich Rechtsgrundlagen zur Datenübermittlung von nichtsensiblen wie auch von sensiblen personenbezogenen Daten existieren, ist allerdings noch nicht die Frage beantwortet, ob die DSGVO an dieser Stelle auch eine Privilegierung im Hinblick auf weitere formelle Anforderungen, insbesondere Verträge, wie sie etwa Art. 26 und Art. 28 DSGVO entspringen, schaffen wollte.

Die Kommentar- und Aufsatzliteratur schweigt dazu beredt an dieser Stelle.

Die einen gehen davon aus, dass auch im Konzernumfeld nicht nur eine Rechtsgrundlage, sondern daneben auch für *jegliche* Datenverarbeitungen bzw. -übermittlungen je nach Art der Datenübermittlung Verträge geschlossen werden müssen, damit die Formalität und Voraussetzung der DSGVO gewahrt seien.[25] Darunter werden auch Binding Corporate Rules nach Art. 47 DSGVO genannt, die an sich – wie gesagt – nur bei der Übermittlung in unsichere Drittstaaten eine Rolle spielen. Aus diesem scheint als Alternative für Datenübermittlungen im Konzern binnen der EU wohl der „Intercompany-Vertrag" entsprungen zu sein, mit dem die ordnungsgemäßen Datenübermittlungen innerhalb von Konzernen auch binnen der EU „dokumentiert" und so der „Nachweispflicht" entsprochen werden soll.

Richtigerweise ist allerdings wohl davon auszugehen, dass innerhalb einer Unternehmensgruppe die Datenübermittlungen ausschließlich auf Art. 6 I f), EG 48 gestützt werden können und als flankierende weitere Schutzmaßnahmen die üblichen nach der DSGVO zu erfüllenden Pflichten wie Informationspflichten nach Art. 12, 13 (Informationen zur Datenverarbeitung gegenüber Mitarbeitern und Kunden), technische und organisatorische Maßnahmen nach Art. 32 bei den jeweiligen Töchtern, das Vorhalten von Datenschutzrichtlinien sowie die entsprechende Dokumentation im Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 ausreichen *können*, um den Dokumentations-, Nachweis und Transparenzpflichten nachzukommen.[26]

---

[25] Rath – Kompendium Kölner Tage Datenschutzrecht, Juni 2019, S. 185 ff.; Kremer, CR 2019, 225, 229; Voigt, Praxisanleitung zur Schaffung eines Konzernprivilegs, CR 2017, 428; Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil 6, Kapitel 1, Rn. 12; Kühling/Buchner – Hartung, DSGVO BDSG, 2. Auflage 2018, Art. 26 Rn. 18.

[26] Haerting, Datenschutzgrundverordnung, 2016, S. 119, Rz. 488; Böhm – DSGVO: Austausch von Mitarbeiterdaten in Konzernen mit Matrixstrukturen, Expertenforum Arbeitsrecht, 22.05.2018, https://efarbeitsrecht.net/mitarbeiterdaten-matrixstrukturen/; Datenschutzbeauftragter INFO – Datenaustausch innerhalb eines Konzerns, 26.10.2018, https://www.datenschutzbeauftragter-info.de/datenaustausch-innerhalb-eines-konzerns-die-interessenabwaegung/; Urban - Konzernprivileg bei AV-Verträgen, 02.11.2018, https://webersohnundscholtz.de/konzernprivileg-auftragsverarbeitungsvertraege/; Ehmann/Selmayr - Selk, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 6 Rn. 25 f. und Art. 88, Rn. 180 ff.; Simitis/Hornung/Spiecker gen. Döhmann - Seifert, Datenschutzrecht, 1. Auflage 2019, Art. 6, 116 und Art. 88, Rn. 177; Bussche v.d./Voigt, Konzerndatenschutz, 2. Auflage 2019, Teil 3, Kap. 3, Rn. 57 sowie insb. zu den flankierenden Maßnahmen Kapitel 6, Rn. 63 ff..; wohl auch: Plath – Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 6, Rn. 89; BeckOK Datenschutzrecht, Wolff/Brink - Albers/Veit, 28. Edition, Art. 6, Rn. 49; Schwartmann/Jaspers/Thüsing – Schwartmann - DSGVO/BDSG, 1. Aufl., Artikel 6, Rn. 142-143.

Der nachfolgende Blick auf das „kleine" Konzernprivileg, die Schutzzweck der DSGVO sowie gesetzlichen Anforderungen an die verschiedenen Kollaborationsformen[27] bei Datenübermittlungen sowie die Praxis zeigt, dass es im Rahmen von Datenübermittlungen im Konzern nur in den wenigsten der Erfüllung weiterer formeller Anforderungen bzw. des Abschlusses weiterer Verträge bedarf.

4.1. Betrachtung des „kleinen" Konzernprivilegs iBa den Schutzzweck

Die DSGVO bezweckt den Schutz der personenbezogenen Daten der Betroffenen. In Folge dessen bedarf es für Datenverarbeitungen stets einer Rechtsgrundlage sowie einer Sicherstellung des Schutzes der betroffenen Daten.

Die DSGVO erlegt den Verantwortlichen insbesondere, aber nicht ausschließlich, über Art. 32 DSGVO die Verpflichtung auf, durch die Einhaltung von technischen und organisatorischen Maßnahmen ist für den Schutz der Daten Sorge zu tragen. Ferner sind die Betroffenen über die jeweiligen Datenverarbeitungen einschließlich der Rechtsgrundlagen und Empfänger nach Art. 12, 13 DSGVO zu informieren.

Tauschen zwei Verantwortliche Daten mit untereinander aus, bedarf jeder Verantwortliche für die Übermittlung bzw. für die dann erfolgte Datenverarbeitung einer Rechtsgrundlage. Der Schutz der Daten sowie alle weiteren Anforderungen, wie etwa Information der Datenverarbeitung, muss grundsätzlich jeder Verantwortliche in eigener Verantwortung erbringen.

Die DSGVO verlangt jedoch grundsätzlich in zwei Fällen der Verarbeitung von Daten zwischen zwei Parteien vorliegen darüber hinaus regelnde und spezielle Abreden zwischen den Parteien.

Dies zum einen in dem Fall, in dem eine Auftragsverarbeitung vorliegt. Hier ist die Besonderheit, dass die Datenverarbeitung zwar durch den Auftragnehmer durchgeführt wird, aber der Auftraggeber einzig der Verantwortliche der Verarbeitung bleibt. Die Folge ist, dass der Auftraggeber im Außenverhältnis die Verantwortung für diese Datenverarbeitung gegenüber den Betroffenen trägt. Wiederum in Folge dessen muss sich der Auftraggeber gegenüber dem Auftragnehmer soweit absichern, als dass letzterer tatsächliche alle Voraussetzungen der DSGVO einhält. Für diese Absicherung sieht die DSGVO mit Art. 28 DSGVO vor, dass ein entsprechender Vertrag zwischen den Beteiligten wenigstens in einem elektronischen Format abgeschlossen wird.[28]

Zum anderen sieht die DSGVO die Notwendigkeit einer Verabredung zwischen den Parteien in dem Fall vor, in dem eine gemeinsame Verantwortung für die Verarbeitung vorgegeben ist. Eine gemeinsame Verarbeitung im Sinne von Art. 26 DSGVO liegt dann vor, wenn die Parteien gemeinsam über den Zweck und die Mittel der Verarbeitung entscheiden. Hier müssen die Parteien einen Vertrag über die gemeinsame Verantwortung nach Art. 26 DSGVO schließen und mit diesem festlegen, wer etwa für welche Verarbeitungsvorgänge oder für die Information der Betroffenen verantwortlich ist. Hier macht die DSGVO weitaus weniger inhaltliche Vorgaben und verlangt auch keine besondere Form für diese Vereinbarung.[29]

---

[27] Gemeint sind hier die dem Gesetz zu entnehmenden Konstellationen des Verantwortlichen zu Verantwortlichen, der gemeinsamen Verantwortung und der Auftragsverarbeitung.

[28] Siehe dazu im Einzelnen: 4.3.3.
[29] Siehe dazu im Einzelnen: 4.3.2

Sinn und Zweck der Art. 26 und 28 DSGVO ist, dass der Schutz der Betroffenen auch in dem Fall gesichert und gut durchsetzbar sein soll, wenn „Dritte“ (nicht im datenschutzrechtlichen Sinn) seine Daten erhalten und mit diesen Daten von Dritten in gewissen Formen gearbeitet wird. Der Auftraggeber kann und darf seine Verantwortung nicht auf den Auftragnehmer delegieren. Gemeinsam Verantwortliche müssen dafür Sorge tragen, dass entsprechend der gemeinsamen Verantwortung sektoral die entsprechenden Verpflichtungen übernommen werden, so dass beispielsweise der Betroffene mit der Geltendmachung von Rechten nicht ins Leere läuft. Der JCC regelt im Innenverhältnis, wer im Außenverhältnis welche Aufgaben zu übernehmen hat und dementsprechend, wer für welchen Teil im Innenverhältnis haftet.

Im Konzern verhält es sich so, dass zunächst einmal die Mutter als auch jede Tochter die Regelungen der DSGVO einhalten müssen. Dies bedeutet unter anderem, dass jeder Konzernteil ein Verzeichnis von Verarbeitungstätigkeiten im Sinne von Art. 30 DSGVO führen, durch technische und organisatorische Maßnahmen den Datenschutz- und die Datensicherheit nach Art. 32 gewährleisten und seinen übrigen Transparenz- und Dokumentationspflichten nachkommen muss. Zur Transparenzpflicht gehört auch den Betroffenen die Informationen der Datenverarbeitung im Sinne der Art. 12, 13 vorzuhalten. In diesen ist sowohl über etwaige Datenübermittlungen, die Rechtsgrundlagen als auch das Widerspruchsrecht und Kontakt zum Datenschutzbeauftragten des Unternehmens zu informieren. Darüber hinaus kann eine konzernweite Datenschutz-Richtlinie sowohl der Transparenz als auch als organisatorische Maßnahme im Sinne von Art. 32 DSGVO dienen.[30]

In zahlreichen Fällen handelt es sich bei Datenübermittlungen im Konzern im Ergebnis um über Übermittlungen von Verantwortlichem zu Verantwortlichem (Controller-to-Controller, CtC).[31] Für diese Konstellation gibt es keine weiteren Vorschriften in der DSGVO. Jeder Verantwortliche hat seine aus der DSGVO entspringenden Pflichten zu erfüllen. Im Konzern gilt nichts anderes. Der von der DSGVO bezweckte Schutz ist von jedem Konzernteil entsprechend zu erfüllen. Ein zusätzlicher CtC-Contract, denn die Beteiligten überobligatorisch schließen würden, würde keinerlei Mehrwert im Hinblick auf den Schutzzweck bieten. Er könnte nur festhalten, was das Gesetz ohnehin verlangt.

Wenn einer der eher seltenen Fälle – auch dazu sogleich noch mehr[32] – der gemeinsamen Verantwortung innerhalb des Konzerns vorläge, so böte ein gesonderter Vertrag über die gemeinsame Verantwortung (Joint Control Vertrag, JCC) nur dann einen Mehrwert für die Betroffenen, wenn sich Abrede über die Verantwortlichkeiten im Hinblick auf die jeweilige Verarbeitung nicht ohnehin schon aus den Verzeichnissen von Verarbeitungstätigkeiten (VVT), dem die Funktion des Daten-Management-Systems zugleich inhärent ist, ergeben. Dies würde Art. 26 DSGVO deshalb genügen, da eine Mindestform der Vereinbarung nicht vorgeschrieben ist, ein JCC also durch gemeinsame konkludente Zustimmung zur Aufgabenverteilung anhand des VVT möglich wäre.[33] Art. 30 DSGVO erfordert zwar nicht, dass Rechtsgrundlagen von Datenverarbeitungen im VVT benannt werden müssen. Da die Nennung von Rechtsgrundlagen jedoch spätestens unter anderem bei der Erstellung von Informationen zur Datenverarbeitung zwingend erforderlich ist, gebietet es die Effizienz, die VVT derart zu führen, dass sich

[30] Ehmann/Selmayr - Selk, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 88, Rn. 184.;
[31] Im Einzelnen dazu unter 4.2 und 4.3.
[32] Im Einzelnen dazu unter 4.2 und 4.3.
[33] Im Einzelnen dazu unter 4.3.2.2

diese Informationen unmittelbar bezogen auf den jeweiligen Verarbeitungsprozess dem VVT entnehmen lassen. Ebenso gebietet es der Effizienzgrundsatz, in den Fällen, in denen ein Datenverarbeitungssystem jedenfalls in irgendeiner Form gemeinsam genutzt wird, dies so bei der Nutzung eines SaaS-Personalmanagementsystems bereits im VVT die Verantwortlichkeiten festzuhalten. So etwa die Verantwortung der verwendenden Töchter für die jeweiligen Informationen zu Datenverarbeitung. Ein JCC regelt zwar das Innenverhältnis der Beteiligten, wenn die Rechte und Pflichten jedoch anderweitig festgehalten sind,[34] bietet ein JCC im Fall der konzerninternen Datenübermittlung im Hinblick auf den Schutzzweck für die Betroffenen keinen Mehrwert. Er kann ohnehin ungehindert von Verabredungen im Innenverhältnis gegenüber allen Verantwortlichen seine Rechte ausüben (Art. 26 III DSGVO), hierfür haften ihm auch alle Verantwortlichen (§§ 421, 426 BGB)[35].

Gleiches gilt bezüglich des Schutzzwecks für den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Verantwortlicher nach außen ist und bleibt der Auftraggeber. Der AVV regelt ausschließlich das Innenverhältnis der Parteien. Im Hinblick auf den Schutzzweck bietet ein AVV im Fall der konzerninternen Übermittlung für die Betroffenen ebenfalls keinen Mehrwert.

Ein „mehr" an Schutz(zweck) erhält ein Betroffener im Rahmen von Konzernübermittlungen also nicht zwingend dadurch, dass zusätzlich Auftragsverarbeitungsverträge, Verträge über die gemeinsame Verantwortung oder gar übergesetzliche CtC-Verträge geschaffen werden.

4.2. Betrachtung des „kleinen" Konzernprivilegs iBa die Praxis

Dieses Ergebnis bestätigt sich in der Praxis und der Betrachtung von faktischen Arbeitsverteilungen im Konzern.

Beim vielfältigen Datenaustausch binnen Konzernen ist es regelmäßig faktisch kaum möglich, die nahezu unendlichen einzelnen Übermittlungen von Daten jeweils hinsichtlich der Daten- und Betroffenenkategorien sowie ihrer Zwecke konsequent einer der drei von der DSGVO (mittelbar) vorgesehenen rechtlichen Funktionen im Sinne von Art. 26, Art. 28 DSGVO bzw. der Übermittlung von Verantwortlichem zu Verantwortlichem zuzuteilen.

Viele Konzerne verwenden Matrixstrukturen als Organisations- und Strukturprinzip im Unternehmen. Hierbei werden Mitarbeitern ihre Aufgaben und Verantwortlichkeiten vorrangig nach ihrer Geeignetheit zugeteilt und die einzelnen Konzerngesellschaften werden als funktionale Einheit behandelt, in Folge dessen spielen die einzelnen Vertragsbeziehungen der Mitarbeiter eine untergeordnete Rolle.[36] So müssen Bereichsleiter oft der Geschäftsführung einer anderen Tochter oder der Mutter berichten; etwa die IT-Leitung der Tochter A-GmbH dem Geschäftsführer der Tochter IT-GmbH, welche sämtliche IT-Leistungen sämtlichen Töchtern und Enkelinnen der Mutter GmbH zur Verfügung stellt. Allein in diesem Fall werden zwischen der IT-Leitung der A-GmbH und der IT-GmbH zahlreiche personenbezogene Daten im weitesten Sinne ausgetauscht werden. Seien es eigene Beschäftigtendaten, wie etwa im Rahmen von Gehaltsverhandlungen und Feedbackgesprächen, seien es Daten zu den Beschäftigten, die im Rahmen von Projekt- und Strategiegesprächen übermittelt werden aber auch Daten von Kunden, wenn etwa

[34] Siehe dazu im Einzelnen auch unter 4.3.2.2
[35] *Bertermann*, in: Ehmann/Selmayr, 2. Aufl. 2018, Art. 26 R. 16.
[36] Vgl. Voigt, Praxisanleitung zur Schaffung eines Konzernprivilegs, CR 2017, 428, Fn. 4

Probleme einer CRM-Datenbank anhand von Beispielen eruiert werden. All diese Datenverarbeitungen und -übermittlungen müssten nicht nur an sich auf ihren Rechtsgrund geprüft und dokumentiert werden (das muss im Rahmen des VVT ohnehin geschehen), sondern sie müssten auch jeweils einer rechtlichen Funktion im Sinne einer AVV, eines JCC oder CtC zugeordnet werden.

In der Theorie ist das möglich. In der Praxis werden etlichen Datenübermittlungen Doppelfunktionen zu Grunde liegen.

Deutlich wird dies an folgendem weiteren Beispiel: Die IT-GmbH hat ein CRM- und Vertriebstool in Form eines SaaS-Tools bei dem 123-Drittanbieter eingekauft. Das Hosting verbleibt naturgemäß beim Drittanbieter. Die IT-GmbH stellt den Töchtern (A, B, C und D GmbH) das Tool zur Verfügung und nutzt dieses darüber hinaus selbst, da die IT-GmbH sowohl intern seine Verträge darüber abwickelt als auch externe IT-Beratungsleistungen erbringt. Es existieren selbstverständlich Berechtigungskonzepte. Jedoch arbeiten die A und C Tochter jeweils beide in sich ergänzenden Bereichen und auch die IT-GmbH sowie die D-GmbH haben Überschneidungen, so dass auch hier Kunden- und Beschäftigtendaten (interne Ansprechpartner etc.) ausgetauscht und selbst weiterverarbeitet werden. Zu guter Letzt gibt es Schnittstellen zu den Daten aus dem Warenwirtschaftssystem, auf welches ebenfalls alle Töchter zugreifen können und welches on premises bei der IT-GmbH liegt.

Das Zurverfügungstellen der SaaS-Lösung durch die IT-GmbH an die Töchter ließe sich grundsätzlich als Auftragsverarbeitung definieren, wobei die IT-GmbH als Auftragnehmer die 123-GmbH als Unterauftragnehmer einsetzt.

Doch in dem Moment, in dem die IT-GmbH das Tool nicht nur selbst nutzt, sondern auch in Kooperation und im Datenaustausch mit den Töchtern, kann dieses Momentum so kaum mehr gehalten werden. Eine reine weisungsgebundene Verarbeitung im Sinne von Art. 28 DSGVO liegt nicht mehr vor.[37] Und eine gemeinsame Verantwortung scheitert daran, dass die Töchter an der Entscheidung über den Einsatz des gemeinsamen Mittels im Sinne von Art 26 DSGVO in keiner Weise beteiligt waren. Auch ein gemeinsamer Zweck lässt sich nur bei einer Überdehnung begründen, nämlich dann, wenn der Austausch der CRM-Daten schon ein gemeinsamer Zweck wäre.[38] Zurück bliebe in diesem Fall wieder ein Verhältnis von CtC.

Die gleiche Problematik wird ersichtlich, wenn man sich einen weiteren Unternehmensbereich ansieht, der klassischerweise zentral zur Verfügung gestellt wird, nämlich den Bereich Personal. Hier sind unter anderem die folgenden Aktivitäten denkbar:

Oft stellt die Personalverwaltung als SSC im Konzern zentral das Bewerber- und Personalmanagement-System zur Verfügung, welches von der Mutter und den Schwestern genutzt wird. Erstaunlicherweise werden gerade solche Systeme immer wieder als Beispiel für eine gemeinsame Verantwortung genannt. Dabei sind in diesen Fällen die dafür notwendigen Tatbestandsmerkmale nicht erfüllt. Schließlich verfolgt jeder Konzernteil für sich den Zweck, bestmögliche Besetzungen für seine freien Positionen zu erhalten. Die Konzernteile stehen – auch bei einer gemeinsamen Nutzung - insoweit in Konkurrenz zueinander. Folglich liegt gerade kein gemeinsamer Zweck vor. Selbst wenn man nun, in Überdehnung des Tatbestandes, die bestmögliche Besetzung als gemeinsamen Zweck erkennen würde, würde es immer

[37] Siehe hierzu im Einzelnen: 4.3.2
[38] Siehe hierzu im Einzelnen: 4.3.2.1

noch an dem Tatbestandsmerkmal des gemeinsamen Mittels mangeln. Schließlich wird das Personalmanagementsystem als Mittel einseitig von dem SSC für alle weiteren Konzernteile gestellt. Damit handelt es sich vielmehr um eine jeweils eigenverantwortliche Verarbeitung bei Nutzung eines gemeinsamen Tools.

Daneben könnte das SSC zentral damit beauftragt sein, den händischen Eintrag aller Papier- und Email-Bewerbungen aller Konzerntöchter von Auszubildenden in das Bewerber-Management-System vorzunehmen. Wenn im Rahmen von Berechtigungskonzepten nur ein Zugriff auf die einzelnen Bewerber von denjenigen Töchtern vorläge, denen die Bewerbung zuging, könnte diese Tätigkeit insoweit als reine Auftragsverarbeitung qualifiziert werden. Regelmäßig wird jedoch entweder unmittelbar die Einwilligung von den Bewerbern eingeholt, die Bewerbungsdaten anderen Töchtern im Rahmen des Talentpools zur Verfügung zu stellen oder die Datenübermittlung wird unter § 26 BDSG iVm EG 48 subsumiert und die Bewerber im Rahmen der Informationen zur Datenverarbeitung eben hierüber aufgeklärt. Hierbei kann es sich um eine reine Auftragsverarbeitung handeln. Schon liegt diesbezüglich wieder eine Verarbeitung in jeweils eigener Verantwortung bei Nutzung einer von der Tochter Personal vorgegebenen gemeinsamen Plattform vor. Eine Trennung der Verarbeitungsvorgänge wäre theoretisch möglich, praktisch jedoch künstlich und kaum darzustellen.

In der Praxis verschwimmen all diese und noch viele Formen mehr der Personalarbeit.

Sowohl innerhalb von Matrix-Strukturen als auch bei der Zentralisierung von Leistungen in Form von Shared Services bedürfen Unternehmensgruppen der Möglichkeit des Datenaustausches von Kunden (z.B. über CRM-Systeme) und Beschäftigtendaten (z.B. hinsichtlich der Fähigkeiten von Mitarbeitern)[39] – und zwar ohne, dass vor lauter bürokratischer Überzuordnungspflicht eine Dokumentationswüste entsteht, deren Mehrwert vollkommen unverhältnismäßig zum Aufwand ist und – wie bereits dargestellt - auch im Hinblick auf die Schutzzwecke keinerlei Mehrwert bietet.

4.3. Betrachtung der gesetzlichen formellen Anforderungen bei der Datenübermittlung

Vor dem Hintergrund der Schutzzwecke und der in der Praxis real existierenden Zuordnungsproblemen bei den verschiedenen Datenübermittlungen sind weiter die gesetzlichen Anforderungen an Controller-to-Controller-Übermittlungen (CtC), Übermittlungen im Rahmen der gemeinsamen Verantwortung (JCC) und bei Auftragsverarbeitungssituationen (DPA) zu betrachten.

4.3.1. CtC - Controller-to-Controller

Die DSGVO kennt keine besonderen formellen Anforderungen an das Controller-to-Controller-Verhältnis und dies aus gutem Grund. Denn wie schon ausgeführt, muss bei einer Datenübermittlung von Verantwortlichem zu Verantwortlichen, wie etwa bei dem Austausch von personenbezogenen Daten zu vertraglichen Zwecken, jeder Verantwortliche die Vorgaben der DSGVO beachten sowie umsetzen und so den Schutz der Daten, die in seiner Sphäre liegen, gewährleisten.

[39] Vgl. dazu: Simitis/Hornung/Spiecker gen. Döhmann – Schantz, Datenschutzrecht, 1. Auflage 2019, Art. 6, Rn. 116, die exakt diese Beispiele von Art. 6 I f) iVm EG 48 gedeckt sehen; Ehmann/Selmayr - Selk, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 88, Rn. 172.

Anders verhält sich dies nur, wenn ein CtC-Verhältnis begründet wird, bei dem Daten in einen unsicheren Drittstaat übermittelt werden. Hier sieht die DSGVO vor, dass für die Übermittlungen in den unsicheren Drittstaat Schutzmaßnahmen dergestalt ergriffen werden, dass für die Datenverarbeitung in dem Drittstaat das gleiche Schutzniveau wie unter der DSGVO erreicht wird. Dies kann zum Beispiel durch einen EU-Standardvertrag Set I oder Set II, Controller to Controller, im Sinne von Art. 46 Abs. 2 c) DSGVO erreicht werden.

Binnen der Jurisdiktion der EU sind CtC-Verträge jedoch nicht notwendig. Der Inhalt eines solchen Vertrages wäre auch redundant, da im Ergebnis der Inhalt der DSGVO wiedergegeben würde. Dies schließt auch bereits die Haftung ein. Wenn hierzu abweichende Regelungen getroffen würden, etwa im Hinblick auf bestimmte Verantwortlichkeiten, wäre dies grundsätzlich wohl möglich, es würde aber unter Umständen gar nahelegen, dass es sich eben nicht um ein CtC-Verhältnis handeln würde.

4.3.2. JCC - Verträge über gemeinsame Verantwortung nach Art. 26 DSGVO

Im Hinblick auf Verträge über die gemeinsame Verantwortung – die derzeit scheinbar „im Trend" liegen, ist zweierlei genauer zu betrachten. Zum einen die Voraussetzungen der gemeinsamen Verantwortung nach Art. 26 Abs. 1 S. 1 DSGVO sowie die formellen Anforderungen bei gemeinsamen Zusammenarbeit nach Art. 26 Abs. 1 S. 2 DSGVO.

4.3.2.1. Gemeinsam Mittel und Zwecke nach Art. 26 DSGVO

Der Wortlaut des Art. 26 Abs. 1 ist insoweit eng gefasst, als er verlangt, dass Zweck „**und**" Mittel gemeinsam festgelegt werden müssten. Eine gemeinsame Verantwortlichkeit liegt also überhaupt nur dann vor, wenn *kumulativ Zwecke und Mittel* der Verarbeitung zusammen festgelegt werden.[40] Eine gemeinsame Verantwortlichkeit ist danach nicht gegeben, wenn zwei Verantwortliche gemeinsam etwa nur die Mittel, jedoch nicht die Zwecke festlegen oder vice versa.[41] Auch Erwägungsgrund 79 verlangt für eine gemeinsame Verantwortlichkeit, dass sowohl die Zwecke als auch die Mittel der Verarbeitung gemeinsam festgelegt werden. Eine gemeinsame Verantwortung kommt darüber hinaus nur in Betracht, wenn eine bewusste *gemeinsame, wesentliche Entscheidung* der Verantwortlichen hinsichtlich Zwecks und Mittel getroffen wurde, eine rein faktische oder gar zufällige Zusammenarbeit reicht nicht aus.[42]

4.3.2.1.1. Praxisbespiele

Obwohl das Vorstehende in nahezu jedem Kommentar konstatiert wird, wird gleichwohl beinahe ständig – insbesondere in Konzernstrukturen - davon ausgegangen, dass regelmäßig eine gemeinsame Verantwortung vorläge,[43] etwa bei Shared Service Centern.

Dabei wird übersehen, dass in zahlreichen Fällen entweder kein gemeinsamer Zweck vorliegt oder aber keine gemeinsame Entscheidung über die Mittel getroffen wurde. Wie oben schon ausgeführt, wird im Hinblick auf Personalmanagementsysteme oder CRM-Datenbanken regelmäßig nicht gemeinsam über die

[40] Gola – Piltz, DSGVO, 2. Auflage 2018, Art. 26, Rn. 3.
[41] Kühling/Buchner - *Hartung*, Art. 26 DSGVO Rz. 13;
[42] Ehmann/Selmayr – Bertermann, DSGVO, 2. Auflage 2018, Art. 26, Rn. 10; Kühling/Buchner/*Hartung,* DS-GVO, Art. 26 Rn. 12; Paal/Pauly/*Martini,* DS-GVO, Art. 26 Rn. 21; Gola/*Piltz,* DS-GVO, Art. 26 Rn. 7.
[43] Vgl. Voigt, Praxisanleitung zur Schaffung eines Konzernprivilegs, CR 2017, 428 f; Kühling/Buchner - *Hartung*, Art. 26 DSGVO Rz. 18; Schwartmann/Jaspers/Thüsing – Kremer, DSGVO/BDSG, 1. Auflage, Artikel 26, Rn. 51.

Mittel entschieden, sondern die Mutter oder der zuständige Konzernteil, der dies als Shared Service anbietet, entscheidet über den Einsatz der Mittel, also dessen Anschaffung und Pflege. Und wenn über ein Mittel gemeinsam entschieden wird, so wird oft eben gerade kein gemeinsamer Zweck verfolgt. Werden Online-Assessments etwa konzernweit innerhalb des Bewerbungsprozesses eingesetzt, so besteht noch lange nicht der gemeinsame Zweck der gemeinsamen Personalauswahl und -einstellung.[44]

4.3.2.1.2. EuGH-Urteil „Fashion ID“

Hieran ändert auch das EuGH-Urteil „Fashion ID“ (Az. C-40/17, Urteil vom 29.07.2019) nichts. Der EuGH befasst sich hier zwar unter anderem mit der Frage der gemeinsamen Verantwortung, konkret ob bei der Einbindung eines Social PlugIns auf einer Webseite, eine gemeinsame Verantwortung zwischen Webseitenbetreiber und PlugIn-Anbieter vorliegt und hat dabei auch auf den ersten Blick die Grenzen, ab wann eine solche gemeinsame Verantwortung vorliegt, weit geöffnet. Schließlich erklärt der EuGH, es läge schon deswegen ein gemeinsames Mittel vor, da die Webseitenbetreiber den Button in dem Wissen, dass dieser als Werkzeug zum Erheben und zur Übermittlung von personenbezogenen Daten der Besucher dieser Seite dient, eingebunden hätten.[45] Bezüglich dieser Erhebung und Übermittlung, nicht aber der weiteren Verarbeitung der Daten durch Facebook, läge eine gemeinsame Verantwortung vor. Weiter statuiert der EuGH, es läge schon deswegen ein gemeinsamer Zweck vor, weil beide Parteien ein wirtschaftliches Interesse daran haben bessere Werbung zu schalten.[46] Die Entscheidung ist im Hinblick auf den konkreten Fall nachvollziehbar. Dies jedenfalls dann, wenn die technische Trennung von Erhebung und Übermittlung einerseits sowie der weiteren Verarbeitung andererseits sowie die damit getrennte unterschiedliche rechtliche Bewertung der Verarbeitungsvorgänge angenommen wird, um insoweit den Button als gemeinsame Mittel subsummieren zu können. Weiter ist auch hier der gemeinsame Zweck noch im konkreten Fall nachzuvollziehen, da tatsächlich beide natürlich ein wirtschaftliches Interesse an besserer Werbung vorweisen. Zu kritisieren ist aber die Trennung der Verarbeitungsvorgänge und damit der rechtlichen Bewertungen. Diese ist technisch zwar möglich ist, faktisch liegt jedoch ein Verarbeitungsvorgang vor. Der EuGH hat allerdings nur diesen konkreten Fall entschieden. Dem Urteil lassen sich keine Kriterien entnehmen, mit denen die gemeinsamen Mittel und Zwecke in anderen Fällen bestimmt werden könnten. Damit impliziert der EuGH - leider - einen äußerst weiten Anwendungsbereich der gemeinsamen Verantwortung, der damit mit an Sicherheit grenzender Wahrscheinlichkeit jedoch gar nicht geschaffen werden sollte. Würde die Auslegung des EuGHs in Sachen Fashion-ID auf jedwede Verarbeitung zwischen zwei Parteien unmittelbar übertragen werden, dann würde praktisch jede Verarbeitung zu einer gemeinsamen Verantwortung. Denn (fast) jede Nutzung eines SaaS-Systems ließe sich als gemeinsam genutztes Mittel und (fast) jeder Vertragszweck als gemeinsamer Zweck deklarieren. Dies wäre aber eine Überdehnung der Tatbestandsmerkmale des Art. 26 DSGVO. Dies ist schon daran ersichtlich, dass die DSGVO daneben die Verarbeitung in Form der Auftragsverarbeitung und von

[44] Vgl. dazu die Beispiele unter 4.2
[45] EuGH C-40/17, – „Fashion ID“, Urteil v. 29.07.2019, Rn. 75 u. 77, http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=4886458.
[46] EuGH C-40/17, – „Fashion ID“, Urteil v. 29.07.2019, Rn. 80, http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=4886458.

Verantwortlichem zu Verantwortlichem, wie sich unter anderem aus Art. 46 Abs. 2 c) und den EU-Standardverträgen ergibt, kennt. Diese wären nicht notwendig, wenn „alles" im Ergebnis eine gemeinsame Verantwortung wäre. Nach wie vor muss der konkrete Einzelfall betrachtet und geprüft werden, ob gemeinsame Mittel und Zwecke im Sinne des Artikel 26 DSGVO, wie hier zuvor erläutert – vorliegen. Der EuGH hat mit der Entscheidung C-40/17 keine Kriterien vergeben. Insoweit ist die Entscheidung für die praktische Anwendung bei anderen Fallkonstellation kaum verwertbar. Es ist absehbar, dass diesbezüglich noch weitere Entscheidungen ergehen werden.

Selbstverständlich ist es zwar nicht ausgeschlossen, dass in einer Unternehmensgruppe bei mehreren Einzelunternehmen gemeinsam ein berechtigtes Interesse an einer konkreten Verarbeitung und somit ein gemeinsamer Zweck existiert und gemeinsam über die Mittel bestimmt wurde; dieses muss aber jeweils individuell festgestellt werden.[47]

Und so wird bei genauer Prüfung (und nicht der Überdehnung des Art. 26 DSGVO) gerade innerhalb von Konzernen regelmäßig keine gemeinsame Verantwortung, sondern vielmehr eine Übermittlung von Daten von Verantwortlichem zu Verantwortlichem vorliegen.

4.3.2.2. Formelle Anforderungen des Art. 26 DSGVO

Liegt tatsächlich eine gemeinsame Verantwortung im Konzernumfeld funktionell vor (auf die Bezeichnung durch die Verantwortlichen kommt es nicht an), so ist weiter zu beachten, dass die formellen Anforderungen des Art. 26 nicht sonderlich hoch sind. Gemäß Art. 26 Abs. 1 S. 2 müssen die gemeinsamen Verantwortlichen in einer Vereinbarung in einer transparenten Form festlegen, wer von ihnen welche Verpflichtungen aus der DSGVO erfüllt.

Es gibt hinsichtlich der Form der Vereinbarung keine Vorschriften.[48] Dies bedeutet, dass sich die Vereinbarung sowie die Aufteilung der Verantwortlichkeiten auch aus den Verzeichnissen von Verarbeitungstätigkeiten sowie aus den allgemeinen Konzernaufgaben ergeben *kann*. Die Transparenzanforderung des Art. 26 Abs. 2 S. 2 DSGVO, nämlich „das Wesentliche der Vereinbarung dem Betroffenen zur Verfügung zu stellen", kann damit über die Informationen zur Datenverarbeitung hergestellt werden. Denn ein Aushändigen oder Übermitteln der Vereinbarung oder der wesentlichen Teile davon im Sinne einer Übergabe ist nicht erforderlich.[49]

Dies ist vor dem Hintergrund der – wie aufgezeigt – zuweilen kaum funktionell zur trennenden Verarbeitungsschritte innerhalb eines Konzerns durchaus hilfreich.

Denn selbst wenn bspw. eine Behörde zu dem Ergebnis käme, es läge sektoral bei einer Verarbeitung von Daten eine funktionelle gemeinsame Verantwortung vor, so können sich die Inhalte eines Vertrages über die gemeinsame Verantwortung praktisch aus den jeweiligen VVT der beteiligten Verantwortlichen ergeben und die Informations- und Transparenzpflichten werden über die Informationen zur Datenverarbeitung erfüllt. Die Verpflichtung etwa, wer genau welche Informationspflichten zu erfüllen hat, ergibt sich regelmäßig ebenso aus den festgelegten Konzernabläufen.

[47] Ehmann/Selmayr – Bertermann, DSGVO, 2. Auflage 2018, Art. 26, Rn. 11.
[48] Gola/*Piltz,* DS-GVO, Art. 26 Rn. 14; Veil – Gierschman, DSGVO, Art. 26, Rn. 66.
[49] Vgl. Veil – Gierschman, DSGVO, Art. 26, Rn. 66.

Auch im Hinblick auf die mögliche Innenhaftung, d.h. den Regress eines Verantwortlichen beim anderen Verantwortlichen, sind weitere Vertragsabreden nicht notwendig.

Haftungsregelungen sind grundsätzlich bereits in der DSGVO niedergelegt. [50] Aus Art. 82 Abs. 4 DSGVO folgt, dass jeder Verantwortliche nach außen für den gesamten Schaden haftet und aus Art. 82 Abs. 5 DSGVO, dass der Zahlende berechtigt ist, von den anderen Ersatz zu verlangen, soweit diese für den Schaden verantwortlich sind. Zwar hat eine Vereinbarung nach Art. 26 DSGVO gerade diesbezüglich eine Beweissicherungs- und Zurechnungsfunktion. Denn wie groß der jeweilige Anteil an der Entstehung eines Schadens ist, hängt auch von der internen Verantwortungszuschreibung ab, die sich wiederum in der Vereinbarung gem. Abs. 1 S. 2 wiederfinden soll. [51] Aber eben diese interne Verantwortungszuschreibung kann sich in einem gemeinsamen Verarbeitungsverhältnis auch aus den VVT ergeben.

Vor diesem Hintergrund wäre eine weitere datenschutzrechtliche Vereinbarung, wer welche Pflichten (etwa Informationspflichten) im Konzernverbund hinsichtlich welcher Datenverarbeitung im Rahmen der gemeinsamen Verantwortung, übernimmt, dann redundant, wenn all dies eben grundsätzlich und sauber bereits in den VVT sowie den flankierenden Dokumenten festgehalten und dokumentiert ist.

4.3.3. AVV - Auftragsverarbeitungsverträge nach Art. 28 DSGVO

Bei der Auftragsverarbeitung verhält es sich anders.

Grundsätzlich verlangt Art. 28 Abs. 9 DSGVO, dass ein Vertrag über die Verarbeitung wenigstens im elektronischen Format geschlossen wird.

Nach Artikel 4 Nr. 8 DSGVO ist ein Auftragsverarbeiter *eine […] Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*. Dem gegenüber ist ein Verantwortlicher im Sinne von Art. 4 Nr. 7 eine […] Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten *entscheidet.*

Daraus ergibt sich im Umkehrschluss, dass der Auftragnehmer eben keine eigenen Entscheidungsbefugnisse hinsichtlich der vorliegenden Datenverarbeitung hat und die Auftragsverarbeitung folglich maßgeblich von der Weisungsgebundenheit geprägt ist.[52]

Demgemäß scheidet eine Auftragsverarbeitung dann aus, wenn der Auftragnehmer eigene Interessen unmittelbar an den personenbezogenen Daten verfolgt. Es widerspräche dem weisungsgebundenen Charakter der Auftragsverarbeitung, wenn der Auftragnehmer die Daten entsprechend seiner selbst gesetzten Zwecke verarbeitet. Davon ausgenommen sind natürlich eigene wirtschaftliche Zwecke wie die Vergütung für die Auftragsverarbeitung.[53]

[50] sowie daneben im BGB und den gesellschaftsrechtlichen Vorschriften zur Haftung im GmbH-Konzern.
[51] Veil – Gierschman u.a., DSGVO, Art. 26, Rn. 69, mwN.
[52] Vgl. BeckOK Wolff/Brink - Spoerr, 28. Ed. 1.5.2019, DSGVO Art. 28 Rn. 18.
[53] Vgl. BeckOK Wolff/Brink - Spoerr, 28. Ed. 1.5.2019, DSGVO Art. 28 Rn. 19.

Auch hier gilt wieder, dass es ausschließlich auf die tatsächlichen Verhältnisse und damit auf ein Handeln im Auftrag des Verantwortlichen ohne eigenen Wertungs- und Entscheidungsspielraum ankommt und nicht darauf, ob und wenn ja welche Verträge bezüglich dieser Verarbeitung geschlossen wurden.[54]

All dies entspricht auch den Einordnungen der Artikel-29-Datenschutzgruppe. Nach dieser gibt es für die Einstufung als Auftragsverarbeiter zwei wesentliche Kriterien: Zum einen müsse die Organisation in Bezug auf den Verantwortlichen *rechtlich eigenständig* sein und zum anderen dürfe die Verarbeitung *nur in dessen Auftrag* erfolgen.[55]

Aus dem Vorstehenden ergibt sich, dass eine Auftragsverarbeitung im Sinne des Art. 28 DSGVO zwischen zwei Konzernteilen nur äußerst selten vorkommt. Regelmäßig wird nämlich die Verarbeitung nicht absolut weisungsbefugt von einer Organisation bei der anderen beauftragt sein und/oder es werden auch noch weitere und eigene Zwecke mit der Datenverarbeitung verfolgt und/oder eine Trennung bzw. Isolierung der verschiedenen Zwecke und Verarbeitungsschritte ist – wie oben aufgezeigt – kaum technisch wie praktisch möglich, so dass zwar theoretisch Auftragsverarbeitungsszenarien in einzelnen Vorgängen bestehen würden, es sich in der Gesamtperspektive aber eben nicht um eine Auftragsverarbeitung handelt.

Anders sieht dies aus, wenn ein Konzernteil, in der Regel derjenige, der als Shared Service Center für die IT-Beschaffung und -Administration zuständig ist, bspw. externe SaaS-Applikationen einkauft und für diese externe Datenverarbeitung den Töchtern bzw. Schwestern Nutzungsrechte einräumt. In diesen Fällen tritt das SSC als Auftraggeber des externen Anbieters, welche der Auftragnehmer ist, auf. Aus Sicht der das SaaS nutzenden Tochter/Schwester ist aber das SSC der Auftragnehmer, der wiederum den externen Anbieter als Unterauftragnehmer beauftragt hat. Diese Verarbeitung von Daten durch jeweils einen Dritten lässt sich als Auftragsverarbeitung isolieren – und zwar unabhängig davon, inwieweit die einzelnen Konzernteile wiederum auf das SaaS-Tool zugreifen und diese Daten zu gemeinsamen Zwecken oder in eigener Verantwortung verarbeiten (Ausnahme: Das SSC nutzt dieses Tool auch noch gemeinsam mit den Töchtern/Schwestern/Mutter).

In diesem Fall muss das SSC einen Auftragsverarbeitungsvertrag als AG mit dem SaaS-Anbieter abschließen. Die anderen Konzernteile müssen wiederum einen Auftragsverarbeitungsvertrag als AG mit dem SSC als AN, in dem der SaaS-Anbieter als UAN benannt wird, abschließen.

Das gleiche gilt natürlich für alle anderen externen tatsächlichen Auftragnehmer, die von einem Konzernteil für alle anderen eingekauft und von diesem an die anderen zur Verfügung gestellt werden.

Dies bedeutet, dass die wenigen echten Auftragsverarbeitungsverhältnisse zwischen Konzernteilen identifiziert und dafür gegebenenfalls AVV zur Verfügung gestellt werden müssen.

Ebenso müssen all die Auftragsverarbeitungsverhältnisse mit externen identifiziert und die daraus abgeleiteten internen Auftragsverhältnisse identifiziert werden. Für jedes

[54] VG Bayreuth, Beschluss v. 08.05.2018, Az. B 1 S 18.105, https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-9586.
[55] Stellungnahme 1/2010 der Artikel-29-Datenschutzgruppe zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP 169, 30; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf.

Auftragsverarbeitungsverhältnis mit einem externen Anbieter muss so dann ein AVV entworfen werden, der zwischen dem SSC als AN und den anderen Schwestern/Töchtern als AG zu schließen ist.

4.3.4. Intercompany-Vertrag – die Mutter aller Lösungen?

Nach dem Vorstehenden scheint hier auf den ersten Blick der Entwurf eines „Intercompany Vertrags" hilfreich. Mit einem solchen könnte grundlegend festgelegt werden, wie im Konzern Auftragsverarbeitungsverträge oder Verträge über die gemeinsame Verantwortung oder Controller-to-Controller Konstellationen ausgestaltet sind.

Bei einer näheren Betrachtung wird jedoch schnell deutlich, dass es sich bei einem Intercompany-Vertrag, der alle Vertragskonstellationen abdecken soll, um eine Scheinlösung handelt.

Zunächst einmal gibt es, wie gesagt, in der DSGVO schon keine Controller-to-Controller-Verträge und regelmäßig keinen Grund solche zu erstellen. Dabei sind aber wohl die meisten Verarbeitungen bzw. Übermittlungen im Konzern als Controller-to-Controller Übermittlungen zu definieren, da – wie herausgearbeitet – bei einer näheren Prüfung der jeweiligen Datenverarbeitungen und -übermittlungen, regelmäßig weder eine gemeinsame Verantwortung noch eine Auftragsverarbeitung gegeben ist.

Davon abgesehen, wird bei der als nahezu Allheilmittel angepriesen Lösung des Intercompany-Vertrags scheinbar das Nachfolgende vergessen:

Die Erstellung eines allgemeinen Rahmenvertrags etwa im Hinblick auf Art. 26 und Art. 28 DSGVO und diesen als Intercompany-Vertrag zu bezeichnen, ist theoretisch nicht schwierig. Praktisch müssten jedoch sektoral in diesem Vertrag selbstverständlich gemäß der gesetzlichen Vorgaben die jeweiligen Datenverarbeitungen, einschließlich der Datenübermittlungen, konkret erfasst werden und im Fall der gemeinsamen Verantwortungen dann auch jeweils die Aufgaben und Pflichten der einzelnen Verantwortlichen festgehalten werden. Ergo wären Teile der jeweils nach Art. 26 und Art. 28 wesentlichen Vertragsinhalte dennoch separat festzuhalten und als Anlagenkonvolut[56] dem Intra-Company-Vertrag beizufügen. Einen „one-fits-all"-Ansatz für diese Anlagen wird es aufgrund der jeweils unterschiedlichen Verarbeitungs- und Übermittlungsvorgänge sowie im Fall von gemeinsamen Verarbeitungen aufgrund der unterschiedlichen Pflichtenlagerung nicht geben können. Hinzu kommt, dass jedenfalls diese Anhänge bei Änderungen stets neu angepasst werden müssten.

Wie oben bereits ausgeführt ist der Mehrwert nicht erkennbar. Und zwar weder im Hinblick auf den Schutzzweck noch bezüglich der Transparenz- und Dokumentationspflichten. All diese Dokumentation, die hier in den Anlagenkonvoluten aufgeführt wären, sind alle bereits im VVT nach Art. 30 DSGVO festzuhalten.

Auch hinsichtlich etwaiger Auftragsverarbeitungen bietet sich ein globaler Intercompany-Vertrag nur äußerst bedingt an. Denn auch hier gilt aufgrund der Vorgaben des Art. 28 DSGVO, dass die Betroffenen- und Datenkategorien sowie die Zwecke der Datenverarbeitung exakt aufgeführt werden müssen.

[56] Sei es als tatsächliches Anlagenkonvolut oder als jeweils dezidierte (!) Verweise in das VVT im Rahmen eines Daten-Management-Systems.

Die Wiederholung und erneute Anpassung in einem Intercompany-Vertrag würde in vielerlei Fällen das Entstehen eines Perpetuum Mobile der Konzern-Bürokratie bedeuten, aber keinen Mehrwert in datenschutzrechtlicher oder – technischer Hinsicht bieten.

4.3.5. Fazit – formelle Anforderungen an Datenübermittlungen im Konzern

Wie aufgezeigt sind bei Datenübermittlungen regelmäßig keine weiteren formellen Anforderungen in Form von Verträgen nach der DSGVO notwendig. Eine Ausnahme bilden echte interne oder externe Auftragsverarbeitungsverhältnisse, welche im Konzern aus den vorgenannten Gründen nur außerordentlich selten vorkommen.

4.4. Fazit – Datenübermittlungen im Konzern

Die meisten Datenübermittlungen im Konzern lassen sich auf das (kleine) Konzernprivileg stützen, ohne dass es daneben noch der Erfüllung weiterer formeller Anforderungen in Form von Verträgen zwischen den Beteiligten bedürfte.

Bei dem überwiegenden Teil der Datenübermittlungen im Konzern wird es sich im Ergebnis um Controller-to-Controller-Übermittlungen handeln.[57] Für diese Form der Datenübermittlung zwischen zwei Verantwortlichen sieht die DSGVO keine Verträge vor.[58]

Gegebenenfalls sind einige wenige Datenübermittlungen im Konzern als Datenverarbeitung im Sinne einer gemeinsamen Verantwortung nach Art. 26 DSGVO zu qualifizieren. Aufgrund der geringen formellen Anforderungen des Art. 26 DSGVO sind im Konzern jedoch keine Verträge nach Artikel 26 DSGVO im engeren Sinne notwendig. Die Vorgaben des Art. 26 lassen sich über ordnungsgemäß geführte Verzeichnisse von Verarbeitungstätigkeiten sowie entsprechende Informationen zur Datenverarbeitung für die Betroffenen erreichen.[59]

Eben aufgrund dessen hat der Landesdatenschutzbeauftragte des Saarlandes wohl auch die Übermittlung von Personaldaten an ein Shared Service Center in einem Konzern ausschließlich auf Grundlage des kleinen Konzernprivilegs für rechtmäßig erachtet.[60]

Zwingende Voraussetzung ist hierbei aber, dass die schon genannten Anforderungen der DSGVO sämtlich eingehalten werden. Dies bedeutet vor allem, dass die Datenverarbeitungsvorgänge und -übermittlung für das VVT nach Art. 30 identifiziert sowie dort beschrieben und nebst Rechtsgrundlage festgehalten werden müssen. Weiter sind durch technische und organisatorische Maßnahmen den Datenschutz- und die Datensicherheit nach Art. 32 zu gewährleisten und den übrigen Transparenz- und Dokumentationspflichten nachzukommen. Zur Transparenzpflicht gehört auch den Betroffenen die Informationen der Datenverarbeitung im Sinne der Art. 12, 13 vorzuhalten. In diesen ist sowohl über etwaige Datenübermittlungen, die Rechtsgrundlagen als auch das Widerspruchsrecht und Kontakt zum Datenschutzbeauftragten des Unternehmens zu informieren. Darüber hinaus kann eine konzernweite

[57] Vgl. dazu die Ausführungen unter: 4.2.
[58] Es sei denn, es handelt sich um Datenübermittlungen in unsichere Drittstaaten.
[59] Vgl. hierzu: 4.2 und 4.3.2.2.
[60] Diese Information habe ich von einem befreundeten Konzerndatenschutzbeauftragten erhalten. Nähere Angaben darf ich an dieser Stelle nicht dazu machen.

Datenschutz-Richtlinie sowohl der Transparenz als auch als organisatorische Maßnahme im Sinne von Art. 32 DSGVO dienen.[61]

Die Übermittlungen weitestgehend unter das Konzernprivileg und die vorgenannten Maßnahmen zu ziehen, ist effizient und bietet den Betroffenen dabei nicht weniger Schutz.[62] Effizient ist dies allein deswegen, weil die vorgenannten Voraussetzungen der DSGVO durch die Verantwortlichen erfüllt werden müssen.

Eine Ausnahme zu dem zuvor Gesagten stellen die wenigen echten internen wie externen Auftragsverarbeitungsverhältnisse dar, da für diese die DSGVO ausdrücklich einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 9 DSGVO fordert, welcher wenigstens im elektronischen Format abgeschlossen werden muss. Allerdings finden sich im Konzernumfeld nur sehr selten interne Auftragsverarbeitungsverhältnisse. Auftragsverarbeitungsverhältnisse mit externem Bezug, wie der Einkauf von SaaS-Systemen und deren Zurverfügungstellung nach können in Form von reinen Auftragsverhältnissen hingegen zuweilen vorkommen.[63]

Aufgrund der in der Regel kaum vorhandenen originären Auftragsverarbeitungsverhältnisse – wie ausgeführt -, bietet es sich hier vielmehr an, bezüglich der wenigen identifizierten echten konzerninternen Auftragsverarbeitungsverhältnisse jeweils einen Auftragsverarbeitungsvertrag zu erstellen.

Hinsichtlich der Auftragsverarbeitungsverhältnisse mit externen Anbietern sind die AVV ebenfalls schnell erstellt. Die Datenverarbeitungen müssen sich aus dem VVT des Auftraggebers (SSC) und dem AVV mit dem Drittanbieter ergeben. Diese Datenverarbeitungen werden dann in einen AVV übernommen, den der interne Auftragnehmer (SSC) allen internen Auftraggebern im Hinblick zur Verfügung stellt und dann diese dann zeichnen. Diese Zeichnung kann auch elektronisch, zum Beispiel über das Intranet erfolgen.

5. Datenübermittlung im Konzern in unsichere Drittstaaten

Des Weiteren sieht es die DSGVO als erforderlich an, dass besondere Maßnahmen zum Schutz von Betroffenen vorgenommen werden müssen, wenn Datenübermittlungen außerhalb der EU, also in sogenannte unsichere Drittstaaten erfolgen. Diese Übermittlungen können etwa durch Vorliegen eines Angemessenheitsbeschlusses nach Art. 45 DSGVO, aufgrund von EU-Standardverträgen nach Art. 46 II c) DSGVO oder aufgrund von Binding Corporate Rules nach Art. 47 DSGVO[64] abgesichert werden.

Die gute Nachricht lautet allerdings, dass die Datenübermittlung in solchen Fällen auch nicht wesentlich komplexer wird.

5.4.1. Datenübermittlung unter einem Angemessenheitsbeschluss nach Art. 45 DSGVO

Findet eine Datenübermittlung in einen Staat außerhalb Jurisdiktion der EU statt, bezüglich dessen die EU-Kommission einen Angemessenheitsbeschluss erlassen hat, gelten die obigen Ausführungen entsprechend.

---

[61] Ehmann/Selmayr - Selk, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 88, Rn. 184.;
[62] Vgl. hierzu: 4.1.
[63] Siehe dazu: 4.2 und 4.3.3.
[64] Binding Corporate Rules können je nach Ausgestaltung allerdings auch selbst eine Rechtsgrundlage für Übermittlungen darstellen.

Es bedarf regelmäßig keiner weiteren Verträge mit Ausnahme von ausschließlichen Auftragsverarbeitungsverhältnissen.

Findet die Auftragsverarbeitung im unsicheren Drittstaat statt, ist ein EU-Standardvertrag Controller-Processor abzuschließen.[65] Findet die Verarbeitung unter der Jurisdiktion der EU oder in einem Land, für das ein Angemessenheitsbeschluss erfolgte, statt, ist ein schlichter Vertrag nach Art. 28 DSGVO zu schließen.

Wie ausgeführt gibt es Angemessenheitsbeschlüsse unter anderem bezüglich Japans und (noch) den USA.[66]

5.4.2. Datenübermittlung unter EU-Standardverträgen nach Art. 46 Abs. 2 c) DSGVO

Datenübermittlungen in unsichere Drittstaaten können auch auf Basis von EU-Standard-Verträgen nach Art. 46 Abs. 2 c) DSGVO erfolgen.

Standardverträge gibt es

- für die Datenübermittlung zwischen zwei Verantwortlichen (Controller-to-Controller).
- für den Fall der Auftragsverarbeitung, bei dem der Auftragnehmer die Daten im unsicheren Drittstaat verarbeitet (Controller-to-Processor).

Die Verträge selbst können nur minimal angepasst werden. Jedoch sind hierfür Appendixe zu erstellen, in denen exakt die Datenkategorien, die Betroffenenkategorien sowie die Zwecke und Rechtsgrundlagen der Datenverarbeitung erfasst werden müssen. Normalerweise sind diese den VVT zu entnehmen.

5.4.3. Datenübermittlung unter Binding Corporate Rules nach Artikel 47

Konzerne können sich auch verbindliche interne Datenschutzvorschriften (BCR) geben, welche

- für alle Mitglieder der Unternehmensgruppe rechtlich verbindlich sein müssen,
- den Betroffenen durchsetzbare Rechte in Bezug auf die Verarbeitung der personenbezogenen Daten übertragen
- und den umfassenden inhaltlichen Anforderungskatalog des Art. 47 Abs. 2 entsprechen müssen.

Darüber hinaus sind derartige verbindliche internen Datenschutzvorschriften nur dann wirksam, wenn diese von der zuständigen Aufsichtsbehörde geprüft und genehmigt wurde.

Sind diese Voraussetzungen gegeben, wirken BCR als Rechtsgrundlage für Datenübermittlungen.

Aufgrund der Genehmigungspflicht sind Binding Corporate Rules nur unter einem sehr hohen Aufwand zu erstellen. Sie stellen nur dann sinnvollen Weg für Unternehmen dar, wenn ein Konzern weltweit verschiedenste, komplexe Datenübermittlungen und -verarbeitungen vornimmt, die sich kaum anderweitig abdecken lassen. In diesem Fall können sich Nutzung und Kosten von BCR die Waage halten.

[65] Vgl. Ziffer 5.4.2.
[66] Es bleibt abzuwarten, wie sich dies im Zusammenhang mit dem US-amerikanischen „Privacy Shield“ weiterentwickelt. Ausführungen hierzu würden an dieser Stelle den Rahmen sprengen.

6. Allgemeine Empfehlungen zur Absicherung der Datenübermittlungen im Konzernverbund

Aus den vorstehenden Einordnungen und Erwägungen lassen sich folgende Empfehlungen für Übermittlungen an SSC in der Praxis entwickeln.

6.1. Erstellung eines detaillierten VVT für jeden Konzernteil

Eine detaillierte Aufstellung der eigenen Verarbeitungsprozesse im VVT nach Art. 30 DSGVO einschließlich der jeweiligen Rechtsgrundlagen ist für jede Konzerntochter und die Konzernmutter (Konzernteile) unabdingbar.

Nur auf diese Weise können überhaupt alle relevanten Datenverarbeitungs- und Datenübermittlungsprozesse identifiziert werden.

6.2. Identifikation und Prüfung der Datenübermittlungsprozesse, Vermerke im VVT

Mittels der detaillierten Erstellung des VVT für die jeweiligen Konzernteile müssen die jeweiligen Datenübermittlungsprozesse identifiziert und geprüft werden.

Dabei ist intern zu prüfen, ob Controller-to-Controller Konstellationen, gemeinsame Verarbeitungen oder Auftragsverarbeitungen vorliegen.

Wie ausgeführt, werden regelmäßig nur einige wenige gemeinsame Verarbeitungen und noch weniger Auftragsverarbeitungsverhältnisse im Konzern zu identifizieren sein.

Weder für die Controller-to-Controller Konstellation noch für die gemeinsame Verantwortung sind binnen der EU im Konzern weitere Verträge abzuschließen. Siehe dazu im Einzelnen Ziffer 4.3.1 und Ziffer 4.3.2.

Die Ergebnisse dieser Prüfung müssen allerdings im VVT vermerkt werden.

Zwar müssen laut Artikel 30 DSGVO weder Rechtsgrundlagen für die Verarbeitung noch für die Übermittlung von Daten genannt werden. Wenn das VVT jedoch zeitgleich Dokumentationszwecke bezüglich der Datenüberübermittlung, im Zweifelsfall gar im Hinblick auf Verträge nach Art. 26 DSGVO, erfüllen können soll, sind diese Rechtsgrundlagen hier jeweils sogleich zu nennen und auch knapp zu begründen. Ferner sollte gegebenenfalls statuiert sein, wer von zwei gemeinsam Verantwortlichen etwaige Pflichten nach innen und/oder außen übernimmt. Da diese Prüfungen ohnehin durchgeführt werden müssen, können dessen Ergebnisse auch so gleich im VVT festgehalten werden.

Werden echte Auftragsverarbeitungen erkannt und im Rahmen einer Prüfung festgestellt, so ist zu fragen, ob bereits notwendige Auftragsverarbeitungsverträge vorliegen oder ob solche noch abgeschlossen werden müssen.

6.3. Datenübermittlungsprozesse im Hinblick auf Drittstaaten-Übermittlungen

Bei der Identifikation und Prüfung der Datenübermittlungen muss weiter geprüft und vermerkt werden, ob eine Übermittlung in sogenannte unsichere Drittstaaten vorliegt.

Hierbei sind Mitgliedsstaaten der EU generell nicht als unsicher einzuordnen. Zu beachten ist die weitere Entwicklung im Vereinigten Königreich.

Sofern eine Übermittlung in Nicht-EU-Staaten erfolgen soll, ist zunächst festzustellen, ob für das Zielland ein Angemessenheitsbeschluss der Kommission vorliegt, wie es etwa für Japan der Fall ist. Übermittlungen zwischen diesen Zielländern und den deutschen Konzerntöchtern unterliegen keinen Besonderheiten.

Die USA sind kein EU-Staat. Hier existiert zwar ebenfalls ein Angemessenheitsbeschluss, das sogenannte „Privacy Shield". Dieses steht aber unter heftiger Kritik und droht aberkannt zu werden.

Soweit notwendig sollten bezüglich der Konzerntöchter in unsicheren Drittstaaten und vorsorglich auch mit etwaigen Konzerntöchtern in den Vereinigten Staaten oder im Vereinigten Königreich ein EU-Standardvertrag geschlossen werden.

7. Fazit

Aufgrund des „kleinen" Konzernprivilegs bzw. der Privilegierung bestimmter Datenübermittlungen durch die DSGVO sind umfassende Vertragswerke regelmäßig nicht notwendig.

Den Dokumentations- und Transparenzpflichten kann jedenfalls bei CtC-Verhältnissen aber auch bei den – voraussichtlich wenigen – JC-Verhältnissen durch gut geführte VVT sowie entsprechende Informationen zur Datenverarbeitung nachgekommen werden.

Eine Ausnahme besteht dann, wenn es sich tatsächlich um Auftragsverhältnisse handelt. In diesem Fall müssen entweder Auftragsverarbeitungsverträge nach Art. 28 DSGVO abgeschlossen werden, wenn die Verarbeitung innerhalb der EU stattfindet. Oder es müssen EU-Standardverträge nach Art. 46 Abs. 2 c) DSGVO „Controller-to-Processor" abgeschlossen werden.

Eine weitere Ausnahme besteht dann, wenn Datenübermittlungen in die USA und nach UK stattfinden. Für diesen Fall müssen zwischen den Beteiligten EU-Standardverträge nach Art. 46 Abs. 2 c) DSGVO „Controller-to-Controller" abgeschlossen werden.

Voraussetzung ist jedoch im Ergebnis in jedem Fall ein VVT, aus dem sich die Datenverarbeitungen und -Übermittlungen ersehen lassen.

Hamburg, 10. Mai 2020