Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO XVII

Mitarbeiterdaten im Unternehmensverbund

INHALT

A. Hinweise zur Nutzung der Praxishilfe 6

B. Allgemeines 6
I. Begriff der Unternehmensgruppe 6
II. Verantwortliche Stellen im Unternehmensverbund 6
III. Weitergabe von Mitarbeiterdaten im Unternehmensverbund 7
IV. Transfer von Mitarbeiterdaten im internationalen Unternehmensverbund ... 8

C. Rechtsgrundlagen der Personaldatenverarbeitung im Unternehmensverbund 8
I. Einleitung 8
II. Allgemeine Zulässigkeitsvoraussetzungen 10
1. Übersicht 10
2. Verhältnis zwischen § 26 BDSG und Art. 6 DS-GVO 11
3. Zulässigkeitsvoraussetzungen des § 26 Abs. 1 S. 1 BDSG 11
4. Zulässigkeitsvoraussetzungen des § 26 Abs. 1 S. 2 BDSG 12
5. Zulässigkeitsvoraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO 13
6. Einwilligung 13
7. Weitergabe sensitiver Mitarbeiterdaten 14

D. Die Auftragsverarbeitung 14
I. Allgemeines 14
II. Auswahl eines konzernangehörigen Auftragnehmers 15
III. Anforderungen an den Vertrag 15
IV. Abgrenzung zwischen Auftragsverarbeitung und Übermittlung 16

INHALT

E. Die gemeinsame Verantwortlichkeit 17

F. Unterrichtungspflichten bei der Datenerhebung 17

G. Informationspfichten bei unrechtmäßiger Kenntnis-erlangung von Daten 18

H. Besondere Zulässigkeitsvoraussetzungen beim Drittlandtransfer 18

I. Zulässigkeit der Verarbeitung (Prüfstufe 1) 18

II. Werkzeuge zur Gewährleistung eines angemessenen Datenschutzniveaus (Prüfstufe 2) 19

1. Angemessenheitsbeschluss der Kommission 19

2. Geeignete Garantien (Art. 46 DS-GVO) 19

2.1 EU-Standardvertragsklauseln („Standardschutzklauseln“) 19

2.2 Binding Corporate Rules 20

2.3 Verhaltensregeln und Zertifizierungen 21

3. Ausnahmen für bestimmte Fälle 21

3.1 Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a DS-GVO) 21

3.2 Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 lit. b DS-GVO) 21

3.3 Erforderlichkeit zur Vertragserfüllung mit einem Dritten (Art. 49 Abs. 1 UAbs. 1 lit. c DS-GVO) 22

3.4 Notwendigkeit aus wichtigen Gründen des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d DS-GVO) 22

3.5 Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e DS-GVO) 22

3.6 Auffangtatbestand Art. 49 Abs. 1 UAbs. 2 S. 2 DS-GVO 23

4. Nicht zulässige Offenlegungen (Art. 48 DS-GVO) 23

INHALT

I. Beispiele typischer Mitarbeiterdatenflüsse im Unternehmensverbund 24

I. Allgemeines 24

II. IT-Infrastruktur 24

1. Übergreifende Netzwerkadministration, Service und Support 24

2. Elektronische Kommunikationsverzeichnisse 25

3. Zentraler E-Mail-/Internet-Server 26

3.1 Verhältnis Arbeitgeber und Beschäftigter 26

3.2 Verhältnis Konzernunternehmen und Konzern-Service-Provider 27

4. Helpdesk 27

5. Cloud-Computing 28

III. Personalrecruiting 29

IV. Shared-Service-Center „Human Resources“ 30

V. Zentrale Führungskräftebetreuung und -entwicklung 31

VI. Übermittlung an Matrix-Vorgesetzte 31

VII. Remotezugriffe auf Mitarbeiterdaten 32

VIII. Skill-Management 33

IX. Mitarbeiterbefragung 34

X. Compliance 34

XI. Bonusprogramme 35

XII. Unternehmenstransaktionen 36

Mitarbeiterdaten im Unternehmensverbund

Vermehrt werden unternehmerische Ziele in nationalen und multinationalen Unternehmensverbünden verfolgt und weltweite Datennetze sowie moderne Informations- und Kommunikationstechnologien vereinfachen den Datenaustausch. Im Zuge der Optimierung ihrer Geschäftstätigkeiten sind die Konzerne in wachsendem Maße darauf angewiesen, Mitarbeiterdaten an die konzernangehörigen Unternehmen - häufig auch grenzüberschreitend - zu transferieren.

Angesichts der Tatsache, dass die EU-Datenschutz-Grundverordnung (DS-GVO) ein „Konzernprivileg“ nicht kennt, ist die datenschutzrechtliche Zulässigkeit der Weitergabe von Mitarbeiterdaten im Unternehmensverbund häufig nicht unproblematisch. Vor diesem Hintergrund greift die vorliegende Praxishilfe Grundsatzfragen und typische Personaldatenflüsse unter datenschutzrechtlichen Gesichtspunkten beispielhaft auf, um dem Verantwortlichen unter Zurateziehung des Datenschutzbeauftragten die praktische Umsetzung der einschlägigen rechtlichen Vorgaben zu erleichtern und zugleich einen Beitrag zu mehr Rechtssicherheit in diesem Bereich zu leisten.

A. Hinweise zur Nutzung der Praxishilfe

Diese Praxishilfe besteht aus einem Grundlagenteil, der allgemein in die Rechtsgrundlagen der Personaldatenverarbeitung in Unternehmensgruppen einführt, sowie einem zweiten Teil, der typische Personaldatenflüsse in Unternehmensgruppen unter datenschutzrechtlichen Gesichtspunkten beispielhaft aufgreift. Damit ermöglicht die Praxishilfe sowohl eine grundlegende als auch eine fallbezogene Lektüre. Im Übrigen ist diese Praxishilfe aufgrund der Verweise in das BDSG vorrangig für den deutschen Rechtsanwender konzipiert.

B. Allgemeines

I. Begriff der Unternehmensgruppe

Der Begriff der Unternehmensgruppe ist in Art. 4 Nr. 19 DS-GVO legal definiert. Hiernach handelt es sich um eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Kennzeichnend für das Vorliegen einer Unternehmensgruppe im Sinne der DS-GVO ist damit das Bestehen eines Über-/Unterordnungsverhältnisses zwischen den Unternehmen. Eine nähere Erläuterung dazu, wann ein Unternehmen als herrschend anzusehen ist, enthält ErwG 37 DS-GVO. Herrschend soll demnach ein Unternehmen sein, „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“ (ErwG 37 Satz 1 DS-GVO). Gemäß ErwG 37 Satz 2 DS-GVO soll ein Unternehmen, das die Verarbeitung personenbezogener Daten in ihm angeschlossenen Unternehmen kontrolliert, zusammen mit diesen als eine „Unternehmensgruppe“ betrachtet werden. Entscheidend ist damit nicht ausschließlich, ob eine Beherrschung im gesellschaftsrechtlichen Sinne gegeben ist. Erfasst werden auch faktische Beherrschungsverhältnisse. Ein Solches ist etwa anzunehmen, wenn aufgrund von Verträgen ein bestimmtes Unternehmen berechtigt ist, Richtlinien zur Datenverarbeitung vorzugeben.

Der Konzern ist ein Fall der Unternehmensgruppe nach Art. 4 Nr. 19 DS-GVO. Ein Konzern liegt nach deutschem Recht gemäß § 18 Abs. 1 Satz 1 Hs. 1 AktG vor, sofern ein herrschendes und ein oder mehrere abhängige Unternehmen unter der einheitlichen Leitung des herrschenden Unternehmens zusammengefasst sind. Der Begriff der Unternehmensgruppe ist insofern weiter als der des Konzerns.

Der Begriff der Unternehmensgruppe ist insbesondere insofern bedeutsam, weil ErwG 48 DS-GVO explizit festlegt, dass Verantwortliche in einer Unternehmensgruppe ein berechtigtes Interesse daran haben können, Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln.

II. Verantwortliche Stellen im Unternehmensverbund

Einem Unternehmensverbund, z.B. einem Konzern, gehören typischerweise mehrere rechtlich selbstständige Unternehmen an. Diese sind jeweils eigenständige Verantwortliche i.S.v. Art. 4 Nr. 7 DS-GVO. Letzteres schließt allerdings nicht aus, dass im Rahmen der Zusammenarbeit - etwa bei konzernübergreifenden Projekten - zusätzlich eine weitere, gemeinsame verantwortliche Stelle (Joint Controllership, Art. 26 DS-GVO) entstehen kann.

Es existieren vielfältige Konzernformen und die Konzernstrukturen sind oft dynamisch. Im Hinblick auf die datenschutzrechtliche Zulässigkeit von Datenflüssen stellt die DS-GVO allerdings nicht auf Beherrschungsverhältnisse, sondern allein auf

den Verantwortlichen i.S.v. Art. 4 Nr. 7 DS-GVO ab. Hinsichtlich der datenschutzrechtlichen Verantwortlichkeit kommt es dabei nur auf die rechtliche Selbstständigkeit der Daten verarbeitenden Stelle an. Des Weiteren können im Unternehmensverbund gemeinsame zentrale Dienstleister (gemeinsames Rechenzentrum, Shared-Service-Center etc.) auftreten. Bei einem rechtlich selbstständigen Dienstleister kommt es hinsichtlich der datenschutzrechtlichen Verantwortung darauf an, ob dieser lediglich als weisungsabhängiger Auftragsverarbeiter i.S.v. Art. 28 DS-GVO tätig ist. Ist dies der Fall, so verbleibt die datenschutzrechtliche Verantwortlichkeit grundsätzlich beim Auftraggeber. Ferner ist das rechtliche Konstrukt der gemeinsamen Verantwortlichkeit ebenso zu beachten, wie eine Datenübermittlung an den neuen Datenempfänger.

Teilweise wird angeregt, sich vom Kriterium der rechtlichen Selbstständigkeit einer Konzerngesellschaft zu lösen und vielmehr auf die tatsächlichen Weisungsbefugnisse abzustellen. In der Folge würden dann in vielen Fällen bei der einer Datenweitergabe im Konzern an Mitarbeiter einer Matrix-Organisation keine Übermittlung personenbezogener Daten an einen Dritten vorliegen, wenn der jeweilige Mitarbeiter der Matrix einem Vorgesetzten innerhalb der Matrix zugeordnet wäre.[1] Dies ist jedoch noch keine aufsichtsbehördlich bestätigte Auffassung.

Eine Stellung des Betriebsrats als Verantwortlicher für die mit der Betriebsratstätigkeit einhergehenden Beschäftigtendatenverarbeitung wurde in der der alten Rechtslage abgelehnt, da der Betriebsrat lediglich Teil einer verantwortlichen Stelle sei.[2] Bezogen auf die DS-GVO mehren sich jedoch die Stimmen[3], dass auch der Betriebsrat verantwortlich für die Verarbeitung von Beschäftigtendaten sein kann. Eine Entscheidung der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder steht diesbezüglich noch aus, wobei sich einzelne Aufsichtsbehörden bezüglich der öffentlichen Stellen bereits gegen eine eigene Verantwortlichkeit des Betriebsrats ausgesprochen haben.[4]

III. Weitergabe von Mitarbeiterdaten im Unternehmensverbund

Verantwortliche Stellen im Unternehmensverbund sind im Rahmen der Verfolgung ihrer gemeinsamen unternehmerischen Ziele vielfach auf die Verarbeitung personenbezogener Daten angewiesen. Die Übermittlung wird in der DS-GVO nicht legal definiert. Im Rahmen der Definition der „Verarbeitung“ in Art. 4 Nr. 2 DS-GVO wird die Übermittlung mit einer Offenlegung personenbezogener Daten verbunden. Eine Übermittlung findet statt, wenn personenbezogene Daten im Zuge konzerninterner Datenflüsse im Konzernverbund weitergegeben werden oder diesen beispielsweise zur Einsicht oder zum Abruf bereitgehalten werden.

Da die DS-GVO keine Privilegierung hinsichtlich der Übermittlung von Mitarbeiterdaten an verbundene Unternehmen kennt und Personaldaten grundsätzlich vertraulich zu behandeln sind, bedarf es zur Legitimation einer solchen Übermittlung von Beschäftigtendaten stets eines gesetzlichen Erlaubnistatbestandes. Anzumerken ist aber, dass es vielfach gerade auch im Interesse der Mitarbeiter liegt, dass ihr Beschäftigungsunternehmen (Arbeitgeber) ihre Daten an verbundene Unternehmen weitergibt. Dies kann z.B. aus Karrieregründen oder zur Abwicklung von Bonusprogrammen geschehen.

1 Vgl. Bussche v.d./Voigt, Konzerndatenschutz Teil 3. Rn. 4.
2 Vgl. Pötters/Gola, RDV 2017, 279 (280).
3 Vgl. Kort, NZA 2015, 1345 (1347); LfDI Baden-Württemberg, Tätigkeitsbericht 2018, S. 37.
4 Vgl. BayLfD, Aktuelle Kurz-Information 23: Der Personalrat - Verantwortlicher im Sinne des Datenschutzrechts?, abrufbar unter https://t1p.de/qkre.

IV. Transfer von Mitarbeiterdaten im internationalen Unternehmensverbund

Im Rahmen der Globalisierung hat die Anzahl multinationaler Unternehmensverbindungen stark zugenommen, womit verstärkt auch die grenzüberschreitende Übermittlung von Mitarbeiterdaten einhergeht. Datenschutzrechtlich muss zwischen der Datenweitergabe in EU- bzw. EWR-angehörige Länder und in sog. Drittländer differenziert werden. Im Falle des Drittlandtransfers hat der Verantwortliche, neben der Prüfung des Erlaubnistatbestandes, für die Datenverarbeitung allgemein, hier die Datenweitergabe, auch zu klären, inwieweit beim Empfänger ein angemessenes Datenschutzniveau vorliegt (sog. „2-Stufen-Prüfung"). Die gesetzlichen Anforderungen an das angemessene Datenschutzniveau bzw. mögliche Ausnahmetatbestände, um von einem solchen abzusehen, finden sich in Kapitel V der DS-GVO (vgl. V.).

C. Rechtsgrundlagen der Personaldatenverarbeitung im Unternehmensverbund

I. Einleitung

Die nachfolgende Darstellung beschränkt sich im Wesentlichen auf die datenschutzrechtlichen Aspekte der Personaldatenverarbeitung im Unternehmensverbund. Daneben sind die allgemeinen arbeitsrechtlichen Bestimmungen zu beachten, wie etwa Tarifverträge und Mitbestimmungsrechte. So ist z.B. zu beachten, dass das Outsourcing der Personaldatenverarbeitung jedenfalls insoweit durch den Betriebsrat mitbestimmt sein muss, wie die an den Auftragnehmer delegierte Datenverarbeitung eine Leistungs- oder Verhaltenskontrolle der Mitarbeiter ermöglicht (§ 87 Abs. 1 Nr. 6 BetrVG). D.h. für dieses Mitbestimmungsrecht ist nicht entscheidend, ob eine Überwachung auch tatsächlich stattfindet. Es genügt, dass sie möglich ist bzw. das eingesetzte System hierzu geeignet ist.[5]

Mitbestimmungspflichtig ist aber nur das ausgegliederte Datenverarbeitungsverfahren, nicht die Ausgliederung an sich. Gegebenenfalls empfiehlt sich der Abschluss einer Betriebsvereinbarung zur Legitimierung einer Datenweitergabe im Unternehmensverbund. Gem. § 26 Abs. 4 Satz 1 BDSG ist die Verarbeitung personenbezogener Daten von Beschäftigten, einschließlich besonderer Kategorien personenbezogener Daten, für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen zulässig. Bereits nach altem Recht wurden Kollektivvereinbarungen aufgrund ihrer normativen Wirkung (vgl. § 77 Abs. 4 BetrVG) als eine „andere Rechtsvorschrift" i.S.d. § 4 Abs. 1 BDSG a.F. angesehen.[6]

Von aufsichtsbehördlicher Seite wurden Anforderungen an Mindestinhalte einer Betriebsvereinbarung zum Austausch personenbezogener Mitarbeiterdaten bereits zur alten Rechtslage formuliert.[7] Zu regelnde Punkte waren hierbei:

- Einschlägige Datenkategorien sowie die als notwendig erachteten Verarbeitungsvorgänge
- Rechte der Arbeitnehmer (Widerspruchsrechte, Informationsrechte)
- Regelung der Zugriffsberechtigungen
- Verantwortlichkeiten für die ordnungsgemäße Verarbeitung der Personaldaten
- Regelung der Mitwirkungs- und Überwachungsrechte des Betriebsrats

5 Vgl. BAG, Beschluss vom 27. 1. 2004, Az. 1 ABR 7/03.
6 Vgl. Schwartmann/Jaspers/Thüsing/Kugelmann/Thüsing-Traut Art. 88 Rn. 49.
7 Hessischer Landtag, Drs. 15/4659, S. 18 m.w.N.

>> Gleichartige Datenorganisation, um die einheitliche Umsetzung der unternehmensweiten Regelungen zu gewährleisten

Mit Blick auf die aktuelle Rechtslage bietet es sich an, zusätzliche Regelungspunkte in die Betriebsvereinbarung aufzunehmen. Hierbei kann aus datenschutzrechtlicher Sicht eine Anlehnung an Art. 30 Abs. 1 DS-GVO erfolgen. Ferner sollten Aspekte der Mitarbeiterüberwachung, so z.B. geplante Auswertungen und Reportings berücksichtigt und dokumentiert werden.

Ob Betriebsvereinbarungen den Datenschutz gegenüber der DS-GVO einschränken können, ist umstritten.[8] Der überwiegende Teil der Literatur ist der Ansicht, dass Betriebsvereinbarungen den Datenschutz gegenüber der DS-GVO/dem BDSG nicht einschränken, sondern vielmehr nur präzisieren können.[9] Dies bedeutet, dass im Falle einer von DS-GVO bzw. BDSG abweichenden Regelung innerhalb der Betriebsvereinbarung diese mindestens so weitreichend sein muss, wie es die DS-GVO bzw. das BDSG es vorgeben. Beispielsweise wäre eine Verkürzung[10] der Bearbeitungszeit für Anfragen betroffener Mitarbeiter hinsichtlich der beim Verantwortlichen gespeicherten Daten zu ihrer Person als unzulässig anzusehen.

Ob über eine Betriebsvereinbarung Verschärfungen hinsichtlich der Zulässigkeit der Verarbeitung personenbezogener Daten möglich sind (z.B. ein absolutes Verbot heimlicher Videoüberwachung, die Statuierung eines gerichtlichen Verwertungsverbots für mitbestimmungs- oder datenschutzwidrig erlangtes Beweismaterial oder der Ausschluss jeglicher Verhaltens- und Leistungskontrolle[11]), ist ebenfalls umstritten. Gute Argumente sprechen für eine entsprechende Verschärfungsmöglichkeit.[12]

Ob durch Betriebsvereinbarung nur die Zulässigkeit der Datenverarbeitung geregelt werden kann oder auch weitere datenschutzrelevante Themen, wie z.B. technisch-organisatorische Fragen, ist im Hinblick auf den Wortlaut des § 26 Abs. 4 BDSG unklar. Die Gesetzesbegründung lässt jedoch auf eine weitergehende Regelungsmöglichkeit schließen. Nach dieser soll die Regelung ganz allgemein einen auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutz ermöglichen.[13] Hier dürfte auch der Hauptanwendungsbereich für Kollektivvereinbarungen liegen.[14]

Kollektivvereinbarungen, die bereits vor Anwendung der DS-GVO abgeschlossen wurden, gelten weiter fort und sind nicht gem. Art. 88 Abs. 3 DS-GVO gegenüber der Europäischen Kommission meldepflichtig.[15] Ob sie weiterhin eine taugliche Rechtsgrundlage darstellen, hängt davon ab, ob sie den Anforderungen der DS-GVO genügen, d.h. vor allem angemessene Schutzmaßnahmen i.S.d. Art. 88 Abs. 2 DS-GVO enthalten. Das ist im jeweiligen Einzelfall zu prüfen.

Darüber hinaus kann eine Betriebsvereinbarung als Rechtsgrundlage auch für den Datentransfer ins Drittland dienen, wenn ihre Regelungen zum Datenschutz an den Datenempfänger im Drittland durchgereicht werden, so z.B. indem diese in einem Vertrag oder in einer anderen Unternehmensregelung für verbindlich erklärt werden. Die Betriebsvereinbarung selbst besitzt im Ausland keine unmittelbare Rechtsgültigkeit, so dass es insofern einer zusätzlichen Absprache bedarf.[16] Auch an dieser Stelle ist ein Vergleich mit den Schutzvorgaben des Kapitels V der DS-GVO geboten. Eine Genehmigungspflicht eigener vertraglicher Regelungen wird regelmäßig durch Art. 46 Abs. 3 lit. a DS-GVO ausgelöst.

8 Zur Rechtslage nach BDSG a.F. vgl. Wurzberger, ZD 2017, 258 (261).
9 Vgl. Kort ZD 2017, 319 (322); Paal/Pauly/Pauly DS-GVO Art. 88 Rn. 12; Wurzberger ZD 2017, 258 (263).
10 Vgl. Art. 12 Abs. 3 S. 1 DS-GVO.
11 Vgl. Maschmann, NZA-Beilage 2018, 115 (117).
12 Vgl. Düwell/Brink, NZA 2016, 665 (668); Gola/Pötters/Thüsing, RDV 2016, 57 (59 f.); Kort, DB 2015, 711 (714); ders., ZD 2017, 319 (322); Taeger/Rose, BB 2016, 819 (831); a.A. Maschmann, NZA-Beilage 2018, 115 (117).
13 Vgl. BT-Drucks. 18/11325, S. 98.
14 Vgl. Kühling/Buchner/Maschmann, DS-GVO BDSG, § 26 Rn. 65.
15 Vgl. Gola/Pötters/Thüsing RDV 2016, 57 (58); Moos/Schefzig/Arning/Baumgartner/Gausling, Die neue Datenschutz-Grundverordnung, S. 548.
16 Vgl. Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 2002, Ziffer 4.7.3.

II. Allgemeine Zulässigkeitsvoraussetzungen

1. Übersicht

Gemäß Art. 5 Abs. 1 lit. a DS-GVO muss die Verarbeitung personenbezogener Daten insbesondere rechtmäßig sein.

Bei der Suche nach einer entsprechenden Rechtsvorschrift für den Umgang mit Beschäftigtendaten im Unternehmensverbund ist an sich die vorrangige Geltung der Grundverordnung zu beachten. Durch die Öffnungsklausel des Art. 88 DS-GVO gilt für die Zulässigkeit der Verarbeitung von Beschäftigtendatendaten das BDSG in folgenden Fällen (vgl. § 1 Abs. 4 BDSG):

- Der Verantwortliche oder Auftragsverarbeiter verarbeitet personenbezogene Daten im Inland
- Personenbezogene Daten werden im Rahmen der Tätigkeiten einer inländischen Niederlassung eines Verantwortlichen oder Auftragsverarbeiters verarbeitet
- Der Verantwortliche oder Auftragsverarbeiter ohne Sitz im Inland fällt in den Anwendungsbereich der DS-GVO (vgl. Art. 3 Abs. 2 DS-GVO), so z.B. indem er Betroffenen im Inland Waren oder Dienstleistungen anbietet

Durch den im BDSG weiterhin verankerten Subsidiaritätsgrundsatz ist jedoch die vorrangige Anwendung bereichsspezifischer Normen des Bundes zu beachten, sollten diese den Umgang mit personenbezogenen Daten regeln (vgl. § 1 Abs. 2 BDSG). Diese bereichsspezifischen Normen sind zwar im Zusammenhang mit der Verarbeitung von Beschäftigtendaten im nichtöffentlichen Bereich seltener anzutreffen, können jedoch z.B. Bedeutung bei der Überwachung der Informations- und Kommunikationstechnik am Arbeitsplatz (Telekommunikationsgesetz - TKG) oder der Veröffentlichung von Mitarbeiterfotos (Kunsturhebergesetz - KunstUrhG) erlangen. Zu beachten ist, dass die bereichsspezifische Regelung nur vorrangig ist, wenn eine Tatbestandskongruenz vorliegt, d.h. der geregelte Sachverhalt deckungsgleich ist. Andernfalls ist das BDSG anzuwenden.

Hinsichtlich des Austauschs von Mitarbeiterdaten im Unternehmensverbund kommen als Erlaubnistatbestände in Betracht:

- Betriebsvereinbarungen
- § 26 Abs. 1 Satz 1 BDSG, sofern die Datenverarbeitung für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist
- § 26 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten
- Überwiegende berechtigte Interessen der übermittelnden Stelle nach Art. 6 Abs. 1 lit. f DS-GVO
- Überwiegende berechtigte Interessen des Datenempfängers nach Art. 6 Abs. 1 lit. f DS-GVO
- Eine freiwillige und informierte Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO i.V.m. § 26 Abs. 2 BDSG (i.V.m. Art. 7 DS-GVO, Art. 4 Nr. 11 DS-GVO, ErwG 32)
- Bei besonderen Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) besondere Gründe nach Art. 9 Abs. 2 DS-GVO (z.B. Einwilligung nach § 26 Abs. 3 Satz 2)

Werden Daten an Stellen außerhalb der EU/des EWR weitergegeben, ergeben sich zusätzliche Zulässigkeitsvoraussetzungen (vgl. hierzu nachstehend Ziff. 4.).

Aufgrund der durch die Datenschutz-Grundverordnung bewirkten Harmonisierung gilt hinsichtlich der Weitergabe von Mitarbeiterdaten an Konzernunternehmen im EU-/EWR-Bereich das Prinzip der Gleichbehandlung mit der inländischen Situation. Mithin ist der Austausch von Mitarbeiterdaten zwischen in Deutschland gelegenen verbundenen Unternehmen unter den gleichen Voraussetzungen zulässig, wie der Austausch dieser Daten zwischen einer deutschen Gesellschaft und einem in der

EU/dem EWR gelegenen verbundenen Unternehmen.

Eine Privilegierung der Datenflüsse zwischen verbundenen Unternehmen kennt die Datenschutz-Grundverordnung, wie bereits ausgeführt, nicht. Allerdings erkennt Erwägungsgrund 48 DS-GVO explizit an, dass Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DS-GVO) haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Beschäftigten, zu übermitteln. Insofern ist einerseits zu beachten, dass der ErwG sich auf interne Verwaltungszwecke bezieht, wobei hieraus teilweise ein abstraktes Konzerninteresse abgeleitet wird.[17] Allerdings muss im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO stets das berechtigte Interesse mit den Interessen der betroffenen Personen abgewogen werden. Diese Abwägung ist pro Verfahren, mithin anhand des jeweiligen Zwecks der Verarbeitung, einschließlich der Übermittlung, durchzuführen.

2. Verhältnis zwischen § 26 BDSG und Art. 6 DS-GVO

Mit dem Gesetz zur Anpassung des Datenschutzrechts an die DS-GVO[18] und der damit verbundenen Einführung des § 26 BDSG wurde in Deutschland in Fortführung des Regelungsgehalts § 32 BDSG a.F.[19] eine Spezialnorm im Bereich des Beschäftigtendatenschutzes geschaffen. Nach dem Willen des Gesetzgebers regelt § 26 BDSG als spezialgesetzliche Norm die Verarbeitung personenbezogener Daten im Beschäftigungskontext.[20] D.h. soweit § 26 BDSG Zulässigkeitstatbestände enthält, treten die entsprechenden Regelungen der DS-GVO zurück.[21] Durch die Fortführung des Regelungsgehalts aus § 32 BDSG a.F. möchte der Gesetzgeber die erarbeiteten Grundsätze der Rechtsprechung zum Beschäftigtendatenschutz weiterhin gelten lassen.[22]

Soweit personenbezogene Daten nicht unmittelbar zur Erfüllung arbeitsvertraglicher Rechte oder Pflichten verarbeitet werden, gleichwohl jedoch Verarbeitungsgegenstand im Kontext eines Arbeitsverhältnisses sind, kann der Tatbestand der Interessenabwägung gem. Art. 6 Abs. 1 lit. f DS-GVO als Rechtsgrundlage in Betracht kommen. In der Praxis wird eine Personaldatenverarbeitung im Unternehmensverbund häufig nur über Art. 6 Abs. 1 lit. f DS-GVO zu legitimieren sein.

3. Zulässigkeitsvoraussetzungen des § 26 Abs. 1 Satz 1 BDSG

Beschäftigtendaten dürfen nach § 26 Abs. 1 Satz 1 BDSG erhoben, verarbeitet oder genutzt werden, falls dies im Rahmen der verschiedenen Phasen eines Beschäftigungsverhältnisses, d.h. seiner Begründung, seiner Durchführung oder seiner Beendigung, erforderlich ist. Unter den Beschäftigungskontext fasst das Gesetz i.S.d. § 26 Abs. 8 BDSG unter anderem das vorvertragliche Rechtsverhältnis mit Bewerbern, das Vertragsverhältnis mit Arbeitnehmern und Auszubildenden sowie das nachvertragliche Rechtsverhältnis mit ausgeschiedenen Arbeitnehmern. Zentraler Maßstab des § 26 Abs. 1 Satz 1 BDSG bildet das Merkmal der Erforderlichkeit für die jeweilige Zweckerreichung. Hierbei sind die Grundrechtspositionen und widerstreitenden Interessen zwischen Arbeitgeber und Arbeitnehmer abzuwägen und zu einem Ausgleich zu bringen.[23] § 26 BDSG findet nach seinem Absatz 7 unabhängig

17 Vgl. Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Auflage 2019, Teil 6, Kapitel 1, Rn. 16 m.w.N.
18 Datenschutz-Anpassungs-und-Umsetzungsgesetz EU – DSAnpUG-EU vom 30. Juni 2017.
19 Vgl. Gola, BB 2017, 1462 (1464); Kort, NZA 2018, 1097 (1098); Thüsing/Rombey, NZA 2018, 1105 (1108); Wybitul, NZA 2017, 413 (415).
20 Vgl. BT-Drs. 18/11325, S. 95.
21 Vgl. Gola/Heckmann/Gola, BDSG, § 26 Rn. 8.
22 Vgl. Maschmann, NZA-Beilage 2018, 115 (120).
23 Vgl. BT-Drs. 18/11325, S. 96.

davon Anwendung, ob Beschäftigtendaten automatisiert, dateigebunden, in chronologisch geführten Personalakten oder auf einfachen Notizzetteln erhoben, verarbeitet oder genutzt werden. Folglich unterfallen auch telefonische Anfragen einer Konzernmutter über Beschäftigte der Firmentochter der Regelung des § 26 Abs. 1 BDSG.

Die Verarbeitung personenbezogener Daten im Rahmen des § 26 Abs. 1 Satz 1 BDSG muss der Erfüllung legitimer Vertragszwecke dienen, die auf andere Weise nicht gewahrt werden können. Erlaubt sind demnach Verarbeitungen, die sich unmittelbar aus dem Arbeitsvertrag ergeben.

Folglich sollte aus Gründen der Rechtssicherheit gerade bei Neueinstellungen oder Vertragsänderungen der Umstand der Beteiligung von anderen Unternehmensteilen berücksichtigt werden. So können z.B. so genannte Mobilitäts- oder Flexibilitätsklauseln in den Vertrag mit aufgenommen werden („sog. Konzerndimensionales Arbeitsverhältnis").[24] Es genügt insofern aber auch, dass bei Begründung der vertraglichen Beziehung eine hinreichende Transparenz bzgl. der Datenverarbeitung im Unternehmensverbund gegeben ist. Dies wird insbesondere bei Führungskräften bzw. sog. „High-Potential-Mitarbeitern" (siehe auch nachstehend G.V.) häufig der Fall sein.

4. Zulässigkeitsvoraussetzungen des § 26 Abs. 1 Satz 2 BDSG

§ 26 Abs. 1 Satz 2 BDSG normiert den Spezialfall der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Aufdeckung von Straftaten im Beschäftigungsverhältnis. Dem Arbeitgeber müssen tatsächliche Anhaltspunkte vorliegen, die den Verdacht begründen, dass der Mitarbeiter im Beschäftigungsverhältnis eine Straftat begangen hat. Dieser Umstand ist zu dokumentieren. Straftaten im rein privaten Bereich fallen nicht unter diese Vorschrift.

Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Aufdeckung der Straftat muss grundsätzlich erforderlich sein. Das schutzwürdige Interesse des Beschäftigten am Ausschluss der Ermittlung darf nicht überwiegen, insbesondere dürfen Art und Ausmaß der Aufklärungsmaßnahmen im Hinblick auf den Anlass nicht unverhältnismäßig sein.

Die Vorgaben des § 26 Abs. 1 Satz 2 BDSG betreffen die Datenverarbeitungen, die eine Aufdeckung einer bereits begangenen Straftat bezwecken. Insofern stellt der Gesetzgeber klar, dass die Zulässigkeit von präventiven Maßnahmen zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen (z.B. Verstöße gegen Unternehmensrichtlinien), die im Zusammenhang mit dem Beschäftigungsverhältnis stehen, nach § 26 Abs. 1 Satz 1 BDSG oder ggf. Art. 6 Abs. 1 lit. f DS-GVO zu beurteilen ist.[25] Folglich hat die verantwortliche Stelle den Zweck der Ermittlung selbst festzulegen (präventive oder repressive Maßnahmen) und im Weiteren ihre Ermittlungsmaßnahmen an der einschlägigen Rechtsgrundlage auszurichten.

Bezogen auf einen Unternehmensverbund entfaltet die Vorschrift des § 26 Abs. 1 Satz 2 BDSG beispielsweise Relevanz, wenn eine verantwortliche Stelle bei der Sachverhaltsaufklärung auf die Mitwirkung einer anderen Stelle des Unternehmensverbundes und deren Datenübermittlung angewiesen ist. Dies kann im Übrigen auch im Umgang mit Meldungen im Rahmen des so genannten „Whistleblowings" von Relevanz sein, bei dem die Mitarbeiter angewiesen werden, Verstöße gegen interne Unternehmensrichtlinien über ein besonders gestaltetes Meldeverfahren weiterzugeben. Die jeweilige Meldung kann Auslöser für nachgelagerte Ermittlungen des Arbeitgebers sein. Ist dieses Meldeverfahren konzernübergreifend aufgesetzt, d.h. die Kanäle des Whistleblowings werden in einer zentralen Compliance-Stelle gebündelt, muss sich die Übermittlung personenbezogener Daten an die Compliance-Stelle wiederum an den gesetzlichen Vorgaben messen lassen.

24 Vgl. Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer", Ziff. 6.3.

25 So bereits in der Gesetzesbegründung zu § 32 BDSG a.F. vgl. BT-Drucks. 16/13657, S. 21.

5. Zulässigkeitsvoraussetzungen des Art. 6 Abs. 1 lit. f DS-GVO

Erfolgt eine Datenübermittlung an andere Stellen im Unternehmensverbund, die nicht unmittelbar Zwecken des Arbeitsverhältnisses dient, kann eine Rechtfertigung über Art. 6 Abs. 1 lit. f DS-GVO gegeben sein. Im Rahmen der dort vorzunehmenden Interessenabwägung können u.a. folgende Kriterien für das Vorliegen überwiegender Übermittlungsinteressen des Arbeitgebers sprechen:

- Transparenz der Übermittlungszwecke
- Beteiligung des Betriebsrats/Sprecherausschusses
- Abschluss von Datenschutzverträgen mit dem Datenempfänger
- Vorliegen verbindlicher Konzernregelungen zum Umgang mit Mitarbeiterdaten (Binding Corporate Rules)
- klare Organisationsregelungen (insb. Zugriffsschutz)

Grundsätzlich dürfen nur solche Mitarbeiterdaten verarbeitet und genutzt werden, die zur Verwirklichung legitimer Arbeitgeberinteressen erforderlich sind. Für den Fall einer Datenübermittlung spielt hierbei auch eine Rolle, ob die die Beschäftigtendaten empfangenden Unternehmen mehr Funktionen erhalten sollen, als der datenabgebenden Stelle als Arbeitgeber selbst zustehen. Eine derartige Kompetenzerweiterung dürfte sich in der Regel negativ auf die vorzunehmende Interessenabwägung auswirken.

Ob eine Datenübermittlung an eine Konzerntochter erforderlich ist, sollte ebenfalls die Frage beinhalten, ob die Daten nicht in gleicher Weise anonym oder pseudonymisiert[26] zur Verfügung gestellt werden können, um den jeweiligen Zweck zu erreichen.

6. Einwilligung

Gemäß Art. 6 Abs. 1 lit. a DS-GVO kann die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten auf eine Einwilligung der Betroffenen gestützt werden. Die Verwendung der Einwilligung im Arbeitsverhältnis ist allerdings wegen des Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer unter dem Gesichtspunkt der Freiwilligkeit nicht unproblematisch. Insofern fordert § 26 Abs. 2 BDSG, dass die Freiwilligkeit einer besonderen Würdigung bedarf. Hierbei ist eine bestehende Abhängigkeit im Beschäftigungsverhältnis ebenso zu berücksichtigen, wie die Umstände unter denen die Einwilligung erteilt worden ist.

Eine Einwilligung im Arbeitsverhältnis kann insbesondere dann als zulässig angesehen werden, wenn mit der Datenübermittlung rechtliche oder wirtschaftliche Vorteile für den Mitarbeiter einhergehen oder gleichgelagerte Interessen verfolgt werden (vgl. § 26 Abs. 2 Satz 2 BDSG). Beispielhaft sind in diesem Zusammenhang Qualifizierungsmaßnahmen, Karrierechancen und Bonusprogramme wie z.B. Stock Options zu nennen. Aber auch die Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder die Erlaubnis zur Privatnutzung von betrieblichen IT-Systeme ist als Vorteil für den Beschäftigten zu werten. Gleichgelagerte Interessen können wiederum durch die gemeinsame Herstellung eines betrieblichen Miteinanders vorliegen, so z.B. die Aufnahme in eine Geburtstagsliste oder die Nutzung von Mitarbeiterfotos im Intranet.[27]

Wichtig ist aber, dass für den Betroffenen eine hinreichende Transparenz bzgl. der hierzu erforderlichen Datenübermittlungen besteht. Insofern kann auch bei den immer mehr gebräuchlichen Self-Service-Tools, bei denen der Mitarbeiter selbst entscheiden kann, ob und welche Daten er in das System eingeben möchte, oft von einer Einwilligung ausgegangen werden.

26 Zur Pseudonymisierung vgl. Schwartmann/Weiß, Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen – Ein Arbeitspapier der Fokusgruppe Datenschutz (2018).

27 Vgl. BT-Drs. 18/11325, S. 96.

Bezüglich der Form der Einwilligung kann eine solche im Beschäftigungskontext schriftlich oder elektronisch abgegeben werden. Insofern wurde das Schriftformerfordernis im Zuge des 2. DSAnpUG-EU[28] in § 26 Abs. 2 Satz 3 BDSG um die elektronische Form ergänzt. Andere Formen sollen möglich sein, soweit sie wegen besonderer Umstände als angemessen zu erachten sind. D.h. die Einwilligung bedarf bspw. nicht mehr zwingend der eigenhändigen Namensunterschrift. Konkludente, durch schlüssiges Handeln hervorgerufene Einwilligungserklärungen können ebenfalls zulässig sein, dürfen jedoch nicht mit einer mutmaßlichen oder stillschweigenden Einwilligung verwechselt werden, die als unzulässig anzusehen ist. Konkludente Einwilligungen sind beispielsweise denkbar, wenn ein Mitarbeiter sein Foto in das Firmen-Intranet oder die Firmen-Internetseite hochlädt.[29]

Eine mündliche Einwilligung scheidet regelmäßig aus, da dies einerseits mit der Wertung des § 26 Abs. 2 Satz 3 BDSG nicht in Einklang zu bringen wäre und der Verantwortliche die Einwilligung nicht nachweisen könnte (vgl. Art. 7 Abs. 1 DS-GVO).

Nicht von der Hand zu weisen ist allerdings, dass die Einwilligung ggf. nicht die ideale Rechtsgrundlage für den mit der Zentralisierung einer internationalen HR-Datenbank beispielsweise einhergehenden Datentransfer ist. Dies ergibt sich bereits aus dem Umstand, dass die Einwilligung jederzeit frei widerruflich ist und damit letztlich keine dauerhaft verlässliche Rechtsgrundlage darstellt.

7. Weitergabe sensitiver Mitarbeiterdaten

Sensitive Daten (besondere Kategorien personenbezogenen Daten nach Art. 9 DS-GVO), wie z.B. Daten über die Gesundheit oder die Religionszugehörigkeit, dürfen nur unter Beachtung besonderer Anforderungen erhoben, verarbeitet oder genutzt werden (Art. 9 Abs. 2 DS-GVO).

In Bezug auf die Rechtsausübung des Arbeitgebers mit Blick auf das Arbeitsrecht, aber auch in diesem Zusammenhang bestehender Pflichten ist eine erforderliche Verarbeitung besonderer Kategorien von Beschäftigtendaten nach Art. 9 Abs. 2 lit. b DS-GVO beispielsweise zulässig. Die Abwicklung der Entgeltabrechnung kann der Arbeitgeber daher im Wege der Auftragsverarbeitung (vgl. C. III.) auf einen sorgfältig ausgewählten Dienstleister übertragen.

D. Die Auftragsverarbeitung

I. Allgemeines

In der Rechtslage vor dem 25.05.2018 war die Datenweitergabe an einen Auftragsverarbeiter mit Sitz in der EU bzw. im EWR privilegiert. Nach der gesetzlichen Definition war er als Teil der verantwortlichen Stelle anzusehen.[30] In der Grundverordnung fehlt eine gesetzliche Privilegierung der Datenweitergabe an einen Auftragsverarbeiter expressis verbis, so dass fraglich ist, ob eine solche Datenweitergabe einer Rechtfertigung aus Art. 6 DS-GVO oder Art. 88 DS-GVO i.V.m. § 26 BDSG bedarf. Im Falle einer Verarbeitung besonderer Kategorien personenbezogener Daten wären gar die Anforderungen des Art. 9 Abs. 2 DS-GVO einzuhalten. Dass dies im Ergebnis zu einer Unzulässigkeit verschiedenster Auftragsverarbeitungen führen würde, wäre nicht von der Hand zu weisen. Daher erscheint es sachgerecht, den Privilegierungsgedanken auch in der DS-GVO zu behalten. Begründet werden kann dies damit, dass die Datenweitergabe an den Dienstleister lediglich einen Verarbeitungsschritt einer Verarbeitung gem. Art. 4 Nr. 2 DS-GVO darstellt. Die

28 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU.

29 Vgl. Paal/Pauly/Gräber/Nolden BDSG § 26 Rn. 35.

30 Vgl. § 3 Abs. 8 S. 2 i.V.m. § 3 Abs. 4 Nr. 3 BDSG a.F.

Rechtfertigung der Datenverarbeitung insgesamt beim Verantwortlichen würde daher auch für den Teilschritt der Datenweitergabe an dien Dienstleister gelten.[31] Immerhin ist dieser durch die Vorgaben des Art. 28 Abs. 3 DS-GVO umfassend an die Vorgaben bzw. Weisungen des Verantwortlichen gebunden.

Sollte ein Dienstleister im Drittland mit der Verarbeitung besonderer Kategorien von Beschäftigtendaten beauftragt werden, kann dies ebenfalls über eine Auftragsverarbeitung erfolgen, vorausgesetzt der Arbeitgeber kann die Zulässigkeit der Verarbeitung insgesamt über Art. 9 Abs. 2 DS-GVO begründen. Die Problematik des BDSG a.F., das die Weitergabe an Auftragsverarbeiter außerhalb der EU bzw. des EWR als Übermittlung einstufte, besteht in der DS-GVO nicht mehr. Die Grundverordnung geht sofern von einer Gleichstellung von Auftragsverarbeitern innerhalb der EU bzw. des EWR und solchen in Drittländern aus. Einer Einhaltung der Vorgaben des Kapitels V an den Drittlandstransfer (vgl. Ziff. D. II.) bedarf es jedoch.

II. Auswahl eines konzernangehörigen Auftragnehmers

Die nach Art. 28 Abs. 1 DS-GVO gebotene sorgfältige Auswahl des Auftragsverarbeiters schließt die Vereinbarung einer Auftragsverarbeitung zwischen Unternehmen, die demselben Konzern angehören, nicht aus. Diesbezüglich werden in dem von der ad-hoc-Arbeitsgruppe veröffentlichten Arbeitsbericht „Konzerninterner Datenverkehr" zum BDSG a.F. folgende Ausführungen gemacht:

„[...] die Vorschrift gebietet nicht, dass eine Auswahl unter Wettbewerbsbedingungen oder gar eine Ausschreibung erfolgt. Maßgeblich ist lediglich, dass ein Auftragnehmer ausgewählt wird, der Gewähr dafür bietet, die Anforderungen des § 9 BDSG nebst Anlage einzuhalten und den vorgegebenen Verarbeitungsauftrag zu erfüllen.

Es ist auch nicht generell abzulehnen die Muttergesellschaft eines Konzerns als Auftragnehmer fungiert. Die konzernrechtliche Position als beherrschendes Unternehmen schließt es nicht schlechthin aus, dass die Konzernobergesellschaft partiell eine „dienende Funktion" im Konzern einnimmt und sich insoweit den Weisungen der konzernangehörigen Gesellschaften unterwirft. Maßgeblich ist, dass entsprechende rechtliche Vereinbarungen getroffen wurden (die dann dem Weisungsrecht gemäß Konzernrecht vorgehen) und keine Anhaltspunkte für eine Missachtung vorliegen."

Folglich sind Auftragsverarbeitungen zwischen einer verantwortlichen Stelle in der EU und einem Mutterkonzern im Drittland grundsätzlich möglich. Dies ist in der Praxis beispielsweise häufig beim Hosting sowie dem Betrieb und Support von IT-Lösungen durch eine Muttergesellschaft zugunsten ihrer Tochterunternehmen vorzufinden.

III. Anforderungen an den Vertrag

Art. 28 Abs. 3 Satz 1 DS-GVO setzt einen Vertrag unter Beachtung der Umsetzung der normierten Mindestanforderungen für die Vertragsgestaltung zwischen dem Verantwortlichen und dem Auftragsverarbeiter voraus. In einem Unternehmensverbund ist es jedoch praktisch häufig so, dass Vertragsverhandlungen mit den Dienstleistern nicht von jedem einzelnen Verantwortlichen geführt werden, sondern ein Verbundunternehmen die Vertragsverhandlungen und den Vertragsschluss mit dem Auftragsverarbeiter übernimmt. Beauftragen die anderen Verbundunternehmen den Auftragsverarbeiter dann später schriftlich unter Bezugnahme auf den

31 Vgl. Laue/Kremer/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis § 5 Rn. 12.

geschlossenen Rahmenvertrag - ggf. unter zusätzlicher Regelung unternehmensspezifischer Anforderungen -, können dadurch die Anforderungen des DS-GVO gewahrt werden (zu den inhaltlichen Anforderungen an den Vertrag vgl. das GDD-Muster zur Auftragsverarbeitung).[32]

IV. Abgrenzung zwischen Auftragsverarbeitung und Übermittlung

Die Privilegierung der Auftragsverarbeitung, die darin zu sehen ist, dass Verantwortlicher und Auftragsverarbeiter rechtlich als einheitliche verantwortliche Stelle gesehen werden (vgl. Art. 4 Nr. 10 DS-GVO), resultiert daraus, dass der Auftragsverarbeiter dem Verantwortlichen in einer oder mehreren Phasen des Datenumgangs weisungsgebunden Unterstützung leistet.

Rechtlich anders behandelt werden soll der Fall, dass ein Dienstleister mehr als nur weisungsgebundene Tätigkeiten durchführt. Dies kann insbesondere dann der Fall sein, wenn ihm neben der Datenverarbeitung weitere Aufgaben oder Funktionen übertragen werden oder er ein eigenes (Geschäfts-) Interesse an der Verarbeitung der ihm überlassenen personenbezogenen Daten verfolgt. Hier kann unter Umständen eine durch eine Erlaubnisnorm zu rechtfertigende Datenübermittlung an Dritte gegeben sein.

Die Frage, ob ein Projekt auf Konzernebene oder innerhalb der Unternehmensgruppe im datenschutzrechtlichen Sinne eine Auftragsverarbeitung oder eine Datenübermittlung darstellt, lässt sich stets nur anhand einer Einzelfallbetrachtung entscheiden.[33] Im Rahmen dieser Einzelfallbetrachtung kommt es entscheidend auf das Maß der eigenverantwortlichen Tätigkeit des Dienstleisters an, d.h. auf den Spielraum, der ihm an freier Gestaltungsmöglichkeit hinsichtlich der Datenverarbeitung verbleibt. Ab wann bei einem Dienstleister das Maß an eigener Gestaltungsfreiheit die Grenze zur Verarbeitung personenbezogener Daten zu eigenen Zwecken überschreitet, kann nur in wenigen Fällen pauschal beantwortet werden. Vertragliche Regelungen können hier eine Rolle spielen. Entscheidend dürfte jedoch eine objektive Betrachtung der Rollenverteilung sein.

Eine Auftragsverarbeitung kann grundsätzlich auch dann vorliegen, wenn dem Auftragnehmer weitreichende, auch über die reine Unterstützung bei der Datenverarbeitung hinausgehende Aufgaben übertragen werden. Maßgeblich ist, dass der Verantwortliche die volle Verantwortung für die gesamte Datenverarbeitung beim Dienstleister übernimmt. Mit Blick auf die Definition des Verantwortlichen in Art. 4 Nr. 7 DS-GVO ist wichtig, dass er über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Eine Entscheidungsbefugnis des Dienstleisters über die eingesetzten technisch-organisatorischen Mittel schließt eine Verarbeitung personenbezogener Daten im Auftrag hierbei nicht aus.[34]

Unstreitig ist jedenfalls, dass in Fällen, in denen dem Dienstleister ein ausdifferenzierter Entscheidungsraum zur Aufgabenerfüllung vorgegeben wird, der ihm keinen inhaltlichen Bewertungs- und Ermessensspielraum belässt, eine Auftragsverarbeitung angenommen werden kann. Eine Auftragsverarbeitung scheidet mitunter aus, wenn Kern der geschuldeten Tätigkeit des Dienstleisters nicht in der Verarbeitung personenbezogener Daten besteht, sondern andere Aspekte der Dienstleistung im Vordergrund stehen.[35]

32 https://www.gdd.de/downloads/praxishilfen/ph-iv-mustervertrag_zur_auftragsverarbeitung_ds-gvo-2

33 Nähere Erläuterungen zur Abgrenzung zwischen Auftragsverarbeitung und Datenübermittlung in GDD-Praxishilfe XIV sowie dem DSK Kurzpapier Nr. 13 zur Auftragsverarbeitung.

34 Vgl. Artikel-29-Datenschutzgruppe WP 169, S. 17.

35 Vgl. LDA Bayern, Auftragsdatenverarbeitung nach § 11, S. 3.

E. Die gemeinsame Verantwortlichkeit

Im Kontext der Beschäftigtendatenverarbeitung im Unternehmensverbund ist auch eine gemeinsame Verantwortlichkeit für personenbezogene Daten möglich. Im Sinne der gesetzlichen Definition der „Joint Controller" legen hierbei mehrere Verantwortliche gemeinsam die Zecke und Mittel einer Verarbeitung personenbezogener Daten fest (vgl. Art. 4 Nr. 7 DS-GVO). Daher bedarf es im Rahmen der Feststellung einer gemeinsamen Verantwortlichen zunächst überhaupt der Stellung eines „Verantwortlichen" in Abgrenzung zum Auftragsverarbeiter (vgl. C. III. 4.). Zur Stellung eines Verantwortlichen kommt sodann das Element der „Gemeinschaftlichkeit" hinzu.[36] Der Wortlaut „gemeinsam" ist dabei nicht im Sinne einer gleichwertigen und gleichberechtigten Kontrolle jedes einzelnen Verarbeitungsschritts durch jeden Beteiligten zu verstehen. Vielmehr können die Beteiligten unterschiedlich stark und in unterschiedlicher Weise in die diesbezüglichen Entscheidungen eingebunden werden.[37] Hierbei kann es unschädlich sein, dass ein Verantwortlicher der gemeinsam für die Verarbeitung Verantwortlichen keinen Zugriff auf personenbezogenen Daten hat, den Verarbeitungsvorgang jedoch zumindest organisiert und koordiniert.[38]

Die gesetzlichen Pflichten im Rahmen einer gemeinsamen Verantwortlichkeit sind in Art. 26 DS-GVO geregelt. Hiernach müssen die beteiligten Stellen in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DS-GVO nachkommt. Das Wesentliche der Vereinbarung muss der betroffenen Person transparent gemacht bzw. zur Verfügung gestellt werden. Aus einer gemeinsamen Verantwortlichkeit resultieren daher erweiterte Anforderungen an die Transparenz der Datenverarbeitung gegenüber dem Betroffenen. Daneben bedarf es einer Vereinbarung unter Einhaltung des gesetzlichen Mindestvorgaben an deren Inhalt.

Art. 26 DS-GVO stellt im Übrigen keine Rechtsgrundlage für die Weitergabe personenbezogener Daten zwischen gemeinsam für die Verarbeitung Verantwortlichen dar. Sie ist insofern nicht privilegiert.[39] Die Zulässigkeit der Datenverarbeitung muss entsprechend anhand der Tatbestände der DS-GVO bzw. des BDSG beurteilt werden (vgl. C. II.).

Eine gemeinsame Verantwortlichkeit für Beschäftigtendaten ist im Umfeld der Unternehmensgruppe oder des Konzerns in verschiedenen Konstellationen denkbar, beispielsweise in Gestalt einer zentralisierten Personalentwicklung oder Personalstrategie.

F. Unterrichtungspflichten bei der Datenerhebung

Aus Gründen der Transparenz sind die Bewerber und Mitarbeiter schon bei der Datenerhebung nach Maßgabe von Art. 13 DS-GVO zu unterrichten. Steht bei der Durchführung eines Bewerbungsverfahrens fest, dass die Daten zur Auswertung an einen Personaldienstleister oder zur weiteren Rekrutierung an andere Verbundunternehmen weitergeleitet werden sollen, so ist auch hierüber zu unterrichten (vgl. Art. 13 Abs. 1 lit. e DS-GVO). Sollte der Datenempfänger seinen Sitz in einem Drittland außerhalb der EU oder EWR haben, ist über den Umstand des Drittlandstransfers sowie seiner Absicherung zu informieren (vgl. Art. 13 Abs. 1 lit. f DS-GVO).

36 Vgl. Katheuser/Nabulsi, MMR 2018, 717 (720).
37 Vgl. Artikel-29-Datenschutzgruppe WP 169, S. 18.
38 Vgl. EuGH , Urteil vom 10.07.2018 - C-25/17, Rn. 75.
39 Vgl. Schreiber, ZD 2019, 55 (55) m.w.N.

Werden personenbezogene Daten nicht bei den Beschäftigten, sondern bei Dritten erhoben, sind die gesetzlichen Anforderungen an eine nachträgliche Benachrichtigung zu beachten (vgl. Art. 14 DS-GVO). Die gesetzlichen Anforderungen an die Benachrichtigung entsprechenden weitestgehend denen des Art. 13 DS-GVO, wobei zusätzlich über die Herkunft der Daten zu informieren ist (vgl. Art. 14 Abs. 2 lit. f DS-GVO).

G. Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten

Sollten im Zuge von Datenweitergaben im Unternehmensverbund personenbezogene Daten von Mitarbeitern unrechtmäßig an Dritte übermittelt worden oder auf sonstige Weise Dritten zur Kenntnis gelangt sein, kann sich hieraus eine Mitteilungspflicht für die jeweilige verantwortliche Stelle im Konzern ergeben. Hinsichtlich einer Mitteilungspflicht gegenüber der zuständigen Aufsichtsbehörde gem. Art. 33 DS-GVO bedarf es zunächst einer Verletzung der IT-Schutzziele der Vertraulichkeit, Verfügbarkeit und Integrität und einer damit verbundenen unbefugten Offenlegung von Daten oder einem unbefugten Zugang hierzu (vgl. Art. 4 Nr. 12 DS-GVO). Ferner muss die Datenschutzverletzung voraussichtlich zu einem Risiko für Rechte und Freiheiten natürlicher Personen führen. Dies dürfte häufig (aber nicht zwangsläufig) der Fall sein, wenn besondere Kategorien personenbezogener Daten gem. Art. 9 DS-GVO oder Informationen zu Bankkonten oder Kreditkarten betroffen sind. Eine Benachrichtigung des Betroffenen gem. Art. 34 DS-GVO ist geboten, wenn die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für Rechte und Freiheiten eines oder mehrerer Betroffener führt. Der Frage der Meldepflicht liegt daher eine Prognoseentscheidung des Verantwortlichen zugrunde, für die er rechenschaftspflichtig ist (vgl. ErwG 85 S. 2). Daher sollte die jeweilige Entscheidung ausreichend dokumentiert werden.

H. Besondere Zulässigkeitsvoraussetzungen beim Drittlandtransfer

Sollen Mitarbeiterdaten an in Drittländern gelegene Konzernteile transferiert werden, bedarf es im Regelfall neben den allgemeinen Zulässigkeitsvoraussetzungen auch des Vorliegens eines angemessenen Schutzniveaus bei der datenempfangenden Stelle im Drittland (sog. „2-Stufen-Prüfung“).

I. Zulässigkeit der Verarbeitung (Prüfstufe 1)

Im Rahmen der ersten Prüfstufe des Drittlandtransfers ist danach zu fragen, ob die allgemeinen Zulässigkeitsvoraussetzungen der DS-GVO für die Datenverwendung erfüllt sind. Insbesondere muss eine Rechtsgrundlage für die Datenübermittlung bestehen, die sich beispielsweise aus Art. 6 Abs. 1 DS-GVO, Art. 9 DS-GVO, § 26 Abs. 1 BDSG oder einer Betriebsvereinbarung ergeben kann. Ebenso sind u.U. die gesetzlichen Vorgaben an die Auftragsverarbeitung gem. Art. 28 DS-GVO zu beachten. Aber auch alle weiteren Anforderungen der Grundverordnung sind einzuhalten, so unter anderem bestehende Informationspflichten.

II. Werkzeuge zur Gewährleistung eines angemessenen Datenschutzniveaus (Prüfstufe 2)

Die gesetzlichen Vorgaben an den Datentransfer in ein Drittland im Rahmen der zweiten Prüfstufe finden sich in Kapitel V der Grundverordnung. Grundsätzlich müssen sog. „geeignete Garantien" beim Datenempfänger gem. Art. 46 DS-GVO bestehen bzw. mit diesem abgeschlossen werden. Alternativ kann auch über einen Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 DS-GVO die jeweilige Übermittlung in das Drittland auf der zweiten Prüfstufe legitimiert werden.

1. Angemessenheitsbeschluss der Kommission

Bezüglich folgender Länder hat die EU-Kommission das Vorliegen eines angemessenen Schutzniveaus bestätigt[40]:

- Andorra (ABl. EU v. 21.10.2010, Nr. L 277),
- Argentinien (ABl. EG v. 05.07.2003, Nr. L 168/19),
- Australien (Nur eingeschränkt für Flugpassagierdaten, ABl. EU v. 08.08.2008, Nr. L 213/47)
- Färöer-Inseln (ABl. EU v. 09.03.2010, Nr. L 58),
- Guernsey (ABl. EG v. 25.11.2003, Nr. L 308/27),
- Isle of Man (ABl. EG v. 30.4.2004, Nr. L 151/51 sowie Berichtigung in ABl. EG v. 10.6.2004, Nr. L 208/47),
- Israel (ABl. EU v. 01.02.2011, Nr. L 27/39),
- Japan (ABl. EU v. 19.03.2019, Nr. L 76),
- Jersey (ABl. EU v. 28.05.2008, Nr. L 138),
- Kanada (ABl. EG v. 4.1.2000, Nr. L 2/13),
- Neuseeland (ABl. EU v. 30.01.2013, Nr. L 028),
- Schweiz (ABl. EG v. 25.8.2000, Nr. L 215/1),
- Uruguay (ABl. EU v. 23.08.2012, Nr. L)
- USA (Nur eingeschränkt für Sonderfall „EU-U.S. Privacy Shield", ABl. EU v. 01.08.2016, Nr. L 207 und für Flugpassagierdaten, ABl. EU v. 11.8.2012, Nr. L 215).

Auch die Übermittlung von Personaldaten kann grundsätzlich in den Anwendungsbereich der EU-U.S.-Privacy Shield-Grundsätze[41] fallen. Die im Internet abrufbare Liste (https://www.privacyshield.gov/list) der dem Privacy Shield angehörenden Unternehmen weist insofern gesondert aus, ob sich die Unternehmen gerade auch im Hinblick auf den Schutz von Mitarbeiterdaten dem Privacy Shield angeschlossen haben. Der inländische Auftraggeber hat im Rahmen seiner Pflichten zu prüfen, ob der Dienstleister tatsächlich auf der Liste des US-Handelsministeriums geführt wird.[42]

2. Geeignete Garantien (Art. 46 DS-GVO)

Neben dem Angemessenheitsbeschluss gem. Art. 45 DS-GVO besteht gemäß Art. 46 DS-GVO die Möglichkeit, ein angemessenes Schutzniveau im Drittland über die Verwendung sog. „geeigneter Garantien" herzustellen.

2.1 EU-Standardvertragsklauseln („Standarddatenschutzklauseln")

In der Praxis werden im Kontext der geeigneten Garantien meist die EU-Standardvertragsklauseln der EU-Kommission („Standarddatenschutzklauseln") eingesetzt. Hierzu hat die EU-Kommission zwei allgemeine Standardvertragswerke und ein spezielles

40 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

41 https://www.privacyshield.gov/article?id=9-Human-Resources-Data.

42 https://www.datenschutz-bayern.de/0/privacy_shield/privacy_shield.html.

Standardvertragswerk anerkannt[43], wobei Letzteres den Fall der Auftragsverarbeitung in einem Drittstaat regelt.[44]

Einer besonderen Würdigung bedarf die in der Praxis häufig anzutreffende Konstellation, dass ein Auftragsverarbeiter mit Sitz in der EU oder dem EWR einen Unterauftragsverarbeiter im Drittland einsetzt. Hier stoßen die EU-Standardvertragsklauseln an ihre Grenzen, da der Auftragsverarbeiter als Datenexporteur nicht die verantwortliche Stelle für die Daten ist und die Standardvertragsklauseln daher unanwendbar sind. Behelfen kann sich der Verantwortliche dadurch, dass er mit dem Unterauftragsverarbeiter im Drittland direkt einen EU-Standardvertrag abschließt. Da dies in der Praxis häufig zu Komplikationen führt, zumal oftmals keine schuldrechtliche Bindung zwischen Verantwortlichem und Unterauftragsverarbeiter besteht, kann der Auftragsverarbeiter seitens des Verantwortlichen beauftragt werden, in dessen Auftrag die Standardvertragsklauseln abzuschließen. Ein Beitritt des Auftragsverarbeiters wird hierbei empfohlen.[45]

Eine Übermittlung von Personaldaten kommt grundsätzlich auch auf Grundlage des zweiten allgemeinen Standardvertragswerks in Betracht, das die EU-Kommission im Dezember 2004 genehmigt hat. Soweit die Aufsichtsbehörden die Auffassung zum BDSG a.F. noch vertraten, dieser von der EU-Kommission anerkannte sog. alternative Standardvertrag zum Drittlandtransfer sei grundsätzlich für Arbeitnehmerdaten nicht geeignet (und eventuell ergänzungsbedürftig), da die Haftung und Auskunftspflicht des Datenexporteurs (des deutschen Arbeitgebers) eingeschränkt seien (vgl. hierzu die Entschließung des Düsseldorfer Kreises[46]), muss dieser Standpunkt auch vor dem Hintergrund der Verbindlichkeit von Kommissionsentscheidungen und des Harmonisierungsgedankens kritisch hinterfragt werden. Immerhin hat die Kommission die alternativen Standardvertragsklauseln insgesamt - und nicht etwa beschränkt auf bestimmte Datenarten - als ausreichende Schutzgarantien anerkannt. Den Bedenken der hiesigen Aufsichtsbehörden kann jedenfalls mit entsprechenden Ergänzungen der alternativen Standardvertragsklauseln[47] begegnet werden.

EU-Standardvertragsklauseln, die vor dem 25.05.2018 mit Dienstleister in Drittstaaten verabschiedet wurde, behalten im Übrigen ihre Gültigkeit (vgl. Art. 46 Abs. 5 Satz 2 DS-GVO).

2.2 Binding Corporate Rules

Im internationalen Konzern kann ein angemessenes Datenschutzniveau zudem über den Einsatz von verbindlichen Unternehmensregelungen zum Umgang mit Personaldaten (Binding Corporate Rules - BCR) erreicht werden.[48] Diese Regelungen werden durch eine federführende Aufsichtsbehörde in Kooperation mit weiteren betroffenen Aufsichtsbehörden in Abhängigkeit des Sitzes der jeweiligen Niederlassung der Unternehmensgruppe genehmigt. Ob, neben der Genehmigung durch die federführende Aufsicht, die einzelnen Datenübermittlungen zusätzlich bei den für den Verantwortlichen weiteren zuständigen Aufsichtsbehörde auf lokaler Ebene angezeigt werden müssen bzw. zusätzliche administrative Vorgaben bestehen, ist im Einzelfall zu prüfen. Bezogen auf die Rechtslage unter der EU-Datenschutzrichtlinie hat die EU-Kommission eine Übersicht über bestsehende Anforderungen im Rah-

43 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
44 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087.
45 Vgl. Fallgruppen zur internationalen Auftragsdatenverarbeitung – Handreichung des Düsseldorfer Kreises zur rechtlichen Bewertung vom 28.03.2007 - Fallgruppe B; a.A. LDA Bayern, 8. Tätigkeitsbericht 2017/2018, Ziff. 14.1, das nur den Direktvertrag mit dem Unterauftragsverarbeiter als zulässig ansieht.
46 https://www.bfdi.bund.de/SharedDocs/Publikationen/EntschliessungssammlungErgaenzendeDokumente/PositionspapierApril2007.pdf.
47 Formulierungsvorschläge hierzu vgl. Schmidl, DuD 2008, 258 (259).
48 Ausführlich zu den Binding Corporate Rules: Artikel-29-Datenschutzgruppe, WP 153, 154, 155, 204.

men der Anzeige von verbindlichen Unternehmensregelungen in den Mitgliedstaaten veröffentlicht.[49] Zu beachten ist, dass die Unternehmensregelungen lediglich das angemessene Datenschutzniveau im Unternehmensverbund herstellen können. Mit eingeschalteten Dienstleistern im Drittland müssen ggf. zusätzlich Maßnahmen ergriffen werden.

In jedem Fall gilt: Neben dem Vorliegen eines angemessenen Datenschutzniveaus bedarf es zusätzlich einer materiellen Übermittlungsbefugnis, so z.B. nach Art. 6 DS-GVO oder Art. 88 DS-GVO i.V.m. § 26 BDSG.

2.3 Verhaltensregeln und Zertifizierungen

Neu in der Grundverordnung ist die Möglichkeit, personenbezogene Daten ins Drittland auf Basis einer Verhaltensregel gem. Art. 40 DS-GVO oder eines Zertifizierungsverfahrens gem. Art. 42 DS-GVO zu übermitteln. Solche Verfahren müssen jedoch rechtsverbindliche und durchsetzbare Verpflichtungen zur Durchsetzung der geeigneten Garantien im Drittland beinhalten. Wie diese Garantien auszugestalten sind, lässt die Grundverordnung offen. Anbieten würde sich ein Vertragswerk, dem sich die beteiligten Stellen unterwerfen, das sich an den Garantien der EU-Standardvertragsklauseln zugunsten der Betroffenen orientiert.[50]

Eine weitere Möglichkeit einer Garantie zur Herstellung eines angemessenen Datenschutzniveaus stellen eigene Vertragsklauseln des Verantwortlichen oder Auftragsverarbeiters dar, die jedoch durch die zuständige Aufsichtsbehörde zu genehmigen sind (vgl. Art. 46 Abs. 3 lit. a DS-GVO).

3. Ausnahmen für bestimmte Fälle

Auch ohne geeignete Garantien oder einen Angemessenheitsbeschluss der EU-Kommission kann eine Übermittlung personenbezogener Daten in ein Drittland zulässig sein. Art. 49 DS-GVO sieht hierzu Ausnahmen für bestimmte Fälle vor. Diese Ausnahmen sind jedoch grundsätzlich restriktiv auszulegen, damit die Ausnahme nicht zur Regel wird.[51]

Art. 49 DS-GVO sieht insgesamt acht Möglichkeiten vor, die eine Übermittlung in ein Drittland ohne angemessenes Schutzniveau erlauben. Die nachfolgende Darstellung wird sich auf relevante Fälle im Beschäftigungskontext beschränken.[52]

3.1 Einwilligung (Art. 49 Abs. 1 UAbs. 1 lit. a DS-GVO)

Eine Möglichkeit zur Übermittlung personenbezogener Beschäftigtendaten in ein Drittland ohne ausreichendes Datenschutzniveau stellt die ausdrückliche Einwilligung des Betroffenen dar. Hierbei sind die allgemeinen Anforderungen an die Einwilligung zu beachten (vgl. Art. 4 Nr. 11 sowie Art. 7 DS-GVO) sowie die besondere Berücksichtigung der Freiwilligkeit im Arbeitsverhältnis. Die Einwilligung ist ausdrücklich und für den konkreten Fall abzugeben. Der Betroffene ist dabei über die Risiken des Transfers in ein Land ohne angemessenes Datenschutzniveau, neben den Vorgaben des Art. 13 DS-GVO, zu informieren. Eine Einwilligung durch schlüssiges Handeln ist beim Drittlandstransfer daher ebenso wenig möglich wie ein sog. „Opt-Out".

3.2 Erforderlichkeit zur Vertragserfüllung (Art. 49 Abs. 1 UAbs. 1 lit. b DS-GVO)

Sollte die Übermittlung personenbezogener Daten in das Drittland zur Vertragserfüllung oder im Zuge vorvertraglicher Maßnahmen, die der Betroffene beantragt hat, erforderlich sein, bedarf es keiner weiterer Maßnahmen zur Gewährleistung eines an-

49 https://archiefotc01.archiefweb.eu/archives/archiefweb/20171123111847/http://ec.europa.eu/justice/data-protection/international-transfers/files/table_nat_admin_req_en.pdf.
50 Vgl. Laue/Kremer/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis § 5 Rn. 59.
51 Vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679 vom 25.05.2018, S. 4 m.w.N.
52 Ausführlich zu den Sonderfällen vgl. Koreng/Lachenmann/Weiß, Formularhandbuch Datenschutzrecht, G. VII. **53** Vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018 a.a.O., S. 10.

gemessenen Datenschutzniveaus. Dies setzt einen engen und erheblichen Zusammenhang zwischen der Übermittlung und den Zwecken des Vertrages voraus.[53] Die Zentralisierung der gesamten Gehalts- und Personalverwaltung an die Muttergesellschaft im Drittland stellt nach Auffassung des Europäischen Datenschutzausschusses mangels fehlendem direktem und objektivem Zusammenhang keine Maßnahme dar, die zur erforderlichen Vertragserfüllung im Arbeitsverhältnis erforderlich wäre.[54] Nach anderer Ansicht[55] kommt eine Anwendung der Ausnahme im Beschäftigungsverhältnis nur dann in Betracht, wenn derartige Übermittlungen tatsächlich in dem Arbeitsvertrag zwischen Mitarbeiter und Unternehmen hinreichend deutlich angelegt sind, da nur dann die Übermittlung zur Erfüllung der Pflichten aus dem Arbeitsvertrag erforderlich ist. Hier wird exemplarisch auf Mitarbeiter verwiesen, die spezifisch für Einkaufs- oder Verkaufskontakte mit Drittländern zuständig sind und dieser Umstand aus dem jeweiligen Arbeitsvertrag hirneichend erkennbar ist.

Im Zuge des Art. 49 Abs. 1 UAbs. 1 lit. b DS-GVO ist zudem zu beachten, dass seitens der Aufsichtsbehörden mit Verweis auf Erwägungsgrund 111 nur gelegentliche Übermittlungen möglich sein sollen; eine systematische Übermittlung zählt hierzu nicht.[56]

3.3 Erforderlichkeit zur Vertragserfüllung mit einem Dritten (Art. 49 Abs. 1 UAbs. 1 lit. c DS-GVO)

In den Fällen der Vertragserfüllung mit Dritten ist der Betroffene nicht als Vertragspartei beteiligt. Der Vertragsschluss zwischen der verantwortlichen Stelle und dem Dritten begünstigt ihn aber bzw. ist in seinem Interesse. Eine Versicherung des Mitarbeiters bei einer ausländischen Gesellschaft kann hierunter ebenso gezählt werden, wie eine Reisebuchung bei Dienstfahrten.[57] Von der Ausnahme nicht umfasst ist beispielsweise die Auslagerung der Gehaltsabrechnung.[58]

Auch im Falle der Verträge mit Dritten soll die Übermittlung erforderlicher personenbezogener Daten nur gelegentlich erfolgen (vgl. ErwG 111).

3.4 Notwendigkeit aus wichtigen Gründen des öffentlichen Interesses (Art. 49 Abs. 1 UAbs. 1 lit. d DS-GVO)

Wichtige Gründe des öffentlichen Interesses können aus Sicht des Verantwortlichen eine Übermittlung ins Drittland rechtfertigen. Dies gilt allerdings nur für Gründe, die in Rechtsvorschriften des Unionsrechts oder dem Recht, dem der Verantwortliche unterliegt, verankert sind. Wichtige Gründe des öffentlichen Interesses eines Drittlandes fallen hierunter nicht.[59] Demnach wären einseitige Anfragen einer Behörde wegen Ermittlungen im öffentlichen Interesse des Drittlands unzulässig, so beispielsweise FISA Orders oder National Security Letters, die ihren Ursprung im US-amerikanischen Recht haben.

3.5 Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 49 Abs. 1 UAbs. 1 lit. e DS-GVO)

Eine Datenübermittlung kann ausnahmsweise zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sein. Der in der

53 Vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018 a.a.O., S. 10.
54 Vgl. Ehmann/Selmayr(Zerdick, DS-GVO, Art. 49 Rn. 10 sowie Paal/Pauly/Pauly, DS-GVO, Art. 49 Rn. 13.
55 Lange/Filip in: BeckOK DatenschutzR, 25. Ed. 2018, Art. 49 Rn. 15.
56 Vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018 a.a.O., S. 11.
57 Ehmann/Selmayr/Zerdick DS-GVO Art. 49 Rn. 12.
58 Vgl. Lange/Filip in: BeckOK DatenschutzR, 25. Ed. 2018, Art. 49 Rn. 22f.
59 Vgl. Ehmann/Selmayr/Zerdick DS-GVO Art. 49 Rn. 14 m.w.N.

EU-Datenschutzrichtlinie noch vorhandene Verweis auf „Rechtsansprüche vor Gericht“ ist entfallen, wodurch auch Datenübermittlungen an Behörden sowie Datenübermittlungen zwischen Privaten im Rahmen der obigen Zweckverfolgung nunmehr möglich sind.[60] Damit können beispielsweise auch sog. Pre-Trial-Discovery-Verfahren nach US-amerikanischem Recht unter die gesetzliche Ausnahme fallen. Einschränkungen vermag es bei Anforderungen von Privaten im Vorfeld eines solchen Verfahrens geben.[61]

Die jeweiligen Datenübermittlungen sind jedoch auf das erforderliche Maß zur Ausübung der eigenen Rechte zu beschränken. Da auch die Rechteausübung, -verfolgung oder -verteidigung im Kontext der „Sonderfälle“ des Art. 49 DS-GVO angesiedelt ist, sollten vorrangig Garantien des Art. 46 DS-GVO eingesetzt werden.[62] Ferner ist die Übermittlung anonymisierter oder zumindest pseudonymisierter Daten vorzugswürdig.[63]

3.6 Auffangtatbestand Art. 49 Abs. 1 UAbs. 2. Satz 2 DS-GVO

Liegt einer Übermittlung personenbezogener Daten ins Drittland weder ein Angemessenheitsbeschluss noch eine Garantie gem. Art. 46 DS-GVO zugrunde und ist keine Ausnahme gem. Art. 49 Abs. 1 UAbs. 1 lit. a-g DS-GVO einschlägig, kann eine Übermittlung über den Auffangtatbestand des Art. 49 Abs. 1 UAbs. 2 Satz 2 DS-GVO gestützt werden. Die diesbezüglichen Anforderungen sind jedoch extrem hoch. Insbesondere darf die Übermittlung nicht wiederholt erfolgen, sie muss zur Wahrung zwingender erforderlicher Rechte erforderlich sein (sofern Rechte und Freiheiten des Betroffenen nicht überwiegen) und nur eine begrenzte Zahl betroffener Personen umfassen.[64] Der Europäische Datenschutzausschuss sieht den Auffangtatbestand des Art. 49 DS-GVO beispielsweise dann als erfüllt an, wenn ein Verantwortlicher gezwungen ist, personenbezogene Daten in das Drittland zu übermitteln, um seine Organisation oder seine Systeme vor einem unmittelbar bevorstehenden, schwerwiegenden Schaden oder vor einer empfindlichen Strafe zu schützen, die sein Geschäft erheblich beeinträchtigen würde.[65]

4. Nicht zulässige Offenlegungen (Art. 48 DS-GVO)

Im Falle einer hoheitlichen Anforderung[66] hinsichtlich in der EU verarbeiteter personenbezogener Daten aus einem Drittland heraus, sieht Art. 48 DS-GVO eine Begrenzung dergestalt vor, dass besagte Anforderung auf ein in Kraft befindliches internationales Übereinkommen gestützt werden muss (z.B. in Gestalt eines Rechtshilfeabkommens).[67] Besteht ein solches Abkommen nicht, bleiben die übrigen Möglichkeiten für den Datenexport ins Drittland gem. Kapitel V weiterhin erhalten.[68] Art. 48 DS-GVO hat daher lediglich eine klarstellende Bedeutung dergestalt, dass eine behördliche oder gerichtliche Entscheidung als solche keine Grundlage für die Übermittlung personenbezogener Daten ins Drittland bilden kann.[69]

60 Vgl. Kühling/Buchner/Schröder, DS-GVO Art. 49 Rn. 25; die unabhängigen Datenschutzbeauftragten des Bundes und der Länder, Kurzpapier Nr. 4, S. 4.
61 Kühling/Buchner/Schröder, DSGVO, Art. 48 DSGVO Rn. 13.
62 Vgl. Art.-29-Datenschutzgruppe, WP 158, S. 11.
63 Vgl. Art.-29-Datenschutzgruppe, WP 158, S. 11.
64 Ausführlich hierzu Europäischer Datenschutzausschuss Leitlinien 2/2018 a.a.O, S. 17 ff.
65 Vgl. Europäischer Datenschutzausschuss Leitlinien 2/2018 S. 18.
66 Zur weiteren Auslegung vgl. Paal/Pauly/Pauly DS-GVO BDSG Art. 48 Rn. 5.
67 Vgl. Ehmann/Selmayr, Datenschutz-Grundverordnung, Art. 48 Rn. 7.
68 Vgl. Gola DS-GVO/Klug DS-GVO Art. 48 Rn. 5.
69 Vgl. Albrecht CR 2016, 88 (95).

I. Beispiele typischer Mitarbeiterdatenflüsse im Unternehmensverbund

I. Allgemeines

Die rechtliche Beurteilung von unternehmensweiten Datenströmen kann sich an zentralen Prüfkriterien ausrichten, die vorab der ersten Weitergabe personenbezogener Daten zu durchlaufen sind. Zunächst muss es sich bei der Art der Daten überhaupt um personenbezogene Daten von Beschäftigten im Sinne des § 26 Abs. 8 BDSG handeln, um überhaupt in den Anwendungsbereich des § 26 BDSG zu gelangen. Ferner ist von Bedeutung, ob es sich bei den Daten gar um besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO handelt. Im Weiteren gilt es, einen konkreten Zweck für die Datenübermittlung festzulegen. Mittels dieser Festlegung ist es möglich zu beurteilen, ob sich eine rechtliche Zulässigkeit bereits aus der Erfüllung arbeitsvertraglicher Pflichten (vgl. § 26 Abs. 1 Satz 1 BDSG) ergeben kann.

Des Weiteren ist zu eruieren, an welche Konzernunternehmen diese Daten übermittelt werden bzw. welche Mitarbeiter von anderen Unternehmen auf diese Daten zugreifen können. Wichtig hierbei ist auch, ob auf Seiten des Empfängers Datenweitergaben an weitere Konzernunternehmen oder an Dritte vorgesehen sind. Letztlich ist von Relevanz, wer verantwortliche Stelle für die übertragenen Daten ist und ob diese Verantwortlichkeit durch eine Auftragsverarbeitung beibehalten, über eine Datenübermittlung an die Empfangsstelle abgegeben oder gar eine gemeinsame Verantwortlichkeit vorliegt. Im Falle eines Empfängers personenbezogener Daten mit Sitz in einem Land außerhalb der EU bzw. des EWR ist darüber hinaus zu prüfen, ob eine Datenübermittlung nach Kapitel V der DS-GVO möglich ist.

II. IT-Infrastruktur

1. Übergreifende Netzwerkadministration, Service und Support

Definition:
Zur Administration oder dem Support der technischen Infrastruktur der Unternehmens- und Konzernnetze sind Steuerungsinstrumente bzw. hierzu eingesetzte Applikationen zur übergreifenden Netzwerkverwaltung erforderlich. Hierzu werden für die Administration teilweise Mitarbeiterstammdaten benötigt. Ferner können im Zuge der Steuerung, der Administration und des Supports weitere personenbezogene Daten verarbeitet werden, so bspw. in Log-Dateien.

Rechtliche Grundlagen:
Die technische Infrastruktur gehört zu den Arbeitsmitteln, die der Arbeitgeber den Arbeitnehmern zur Verfügung stellt. Die Verwendung personenbezogener Mitarbeiterstammdaten zur Organisation und Steuerung dieser Systeme ist zur Erfüllung der arbeitsvertraglichen Pflichten und somit auch für die Durchführung des Beschäftigungsverhältnisses erforderlich. Mithin ergibt sich die datenschutzrechtliche Zulässigkeit aus dem Arbeitsvertrag (§ 26 Abs. 1 Satz 1 BDSG).

Bezüglich der Verarbeitung darüber hinaus gehender personenbezogener Daten, etwa in Log-Dateien, wird in vielen Fällen eine Interessenabwägung gem. Art. 6 Abs. 1 lit. f DS-GVO vorgenommen werden müssen. Dies gilt auch, wenn solche Leistungen durch konzerninterne oder externe Dienstleister vorgenommen werden. Auch hier gilt der Maßstab, dass nur erforderliche, mithin für die Zweckerreichung notwendige Daten verarbeitet

werden dürfen.

Ob durch die Einschaltung von Gesellschaften der Unternehmensgruppe im Rahmen der Netzwerkadministration und dem Support eine Datenübermittlung oder eine Auftragsverarbeitung einhergeht, hängt von den Motiven der Beteiligten hierbei ab. Erfolgt die Unterstützung weisungsgebunden und ohne die Verfolgung eigener Ziele der Gesellschaft, ist regelmäßig eine Auftragsverarbeitung gem. Art. 28 DS-GVO anzunehmen. Auch wenn Art. 28 DS-GVO nicht ausdrücklich auf die Fernwartung eingeht (im Gegensatz zu § 11 Abs. 5 BDSG a.F.), sind die Regeln der Auftragsverarbeitung auf diese Fallkonstellation regelmäßig anwendbar.[70] Eine gemeinsame Verantwortlichkeit gem. Art. 26 DS-GVO käme nur dann in Betracht, wenn die beteiligte Gesellschaft gemeinsam mit den anderen Gesellschaften Zwecke bzw. Interessen bezüglich der verarbeiteten personenbezogenen Daten verfolgen würde.[71] Dies wäre denkbar, wenn die mit der Administration und dem Support befasste Gesellschaft Analysen anfallender personenbezogener Log- oder Metadaten vornehmen würde, um die Funktionalität der selbst eingesetzten Tools zu verbessern.

Praxishinweis:
Sollte eine Unternehmensgruppe über eine Vielzahl an Administratoren verfügen, die über mehrere Gesellschaften verteilt sind, empfiehlt sich die Bildung einer einheitlichen Administratorenstelle bei einer Gesellschaft, die als Auftragsverarbeiter für die jeweilige verantwortliche Stelle oder selbst als Verantwortlicher agiert. Eine örtliche Bündelung ist dabei nicht erforderlich. Im Falle einer zentralen Administratorenstelle kann auf den Abschluss einer Vielzahl von Einzelverträgen zwischen den beteiligten Stellen verzichtet werden. Dies kann sich ebenfalls positiv auf etwaige Prüfpflichten hinsichtlich der beim Beteiligten vorherrschenden technisch-organisatorischen Maßnahmen auswirken, da eine zentralisierte Administratorenstelle über technisch-organisatorische Maßnahmen verfügt, die sich an der Kerntätigkeit ausrichten.

Soweit die Administration der IT-Infrastruktur aus einem Drittland heraus vorgenommen wird und hierbei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, gelten die zusätzlichen Zulässigkeitsvoraussetzungen nach Kapitel V der Grundverordnung. Aus Sicht der Praxis wird bei der Netzwerkadministration, Service und Support regelmäßig der Abschluss der EU-Standardvertragsklauseln in der Variante „Controller to Processor“ in Frage kommen. Hierbei können standardisierte administrative Tätigkeiten oder solche des Service u. Supports über ein einziges Vertragswerk vereinbart werden, ohne dass der Abschluss einer Vielzahl von Einzelvereinbarungen notwendig wäre.

2. Elektronische Kommunikationsverzeichnisse

Definition:
Elektronische Kommunikationsverzeichnisse werden zum Zwecke einer effizienten Kommunikation zwischen den einzelnen Konzernunternehmen bzw. deren Mitarbeitern konzernweit - häufig über Intranet - zugänglich gemacht.

Gegenstand der damit einhergehenden Datenübermittlungen sind meist Basiskommunikationsdaten der Mitarbeiter, die in Namens-, Telefon- und E-Mail-Verzeichnisse aufgenommen werden. Häufig erfolgt auch eine Aufnahme zusätzlicher Informationen, wie eine Gesellschaftszugehörigkeit, der betroffene Organisationsbereich sowie eine konkrete Stellenbezeichnung.

Rechtliche Grundlagen:
Um den Konzernzielen gerecht werden zu können,

70 Vgl. die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) Kurzpapier Nr. 13, S. 4; Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, § 5 Rn. 10 weist darauf hin, dass bei Leistungen des Dienstleisters, die nicht zwingend die Verarbeitung personenbezogener Daten bedürfen, keine Auftragsverarbeitung anzunehmen sei.

71 Vgl. GDD-Praxishilfe XV: Die gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO, Ziff. 3.2.

bedarf es regelmäßig der Kommunikation zwischen den Mitarbeitern der einzelnen Konzernteile. Vielfach ergibt sich die Berechtigung zur konzerninternen Übermittlung der erforderlichen Basiskommunikationsdaten der Mitarbeiter bereits aus den ihnen obliegenden arbeitsvertraglichen Pflichten (§ 26 Abs. 1 Satz 1 BDSG).

Werden lediglich die dienstlichen Basiskommunikationsdaten der einzelnen Mitarbeiter in die konzernweiten Kommunikationsverzeichnisse aufgenommen und kann die Datenübermittlung nicht unmittelbar aus den arbeitsvertraglichen Pflichten abgeleitet werden, führt aber auch eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zur Zulässigkeit der damit einhergehenden Datenübermittlungen. Das unternehmerische Interesse an einer effizienten, konzernweiten Mitarbeiterkommunikation überwiegt insoweit Vertraulichkeitsinteressen der Mitarbeiter, soweit solche überhaupt bestehen. Dies ergibt sich insbesondere daraus, dass diese dienstlichen Basiskommunikationsdaten keine besondere Sensitivität aufweisen.

Unter Angemessenheitsgesichtspunkten besteht hinsichtlich der Basiskommunikationsdaten auch kein sachlicher Grund dafür, sich lediglich auf sog. Funktionsträger zu beschränken. Vielmehr kommt es mit Blick auf eine angemessene Technikgestaltung darauf an, dass ein Mitarbeiter aufgabenbezogen in das Verzeichnis aufgenommen wurde bzw. entsprechende Zugriffsrechte erhalten hat.

Sollen über die o.g. Basiskommunikationsdaten hinausgehende Informationen aufgenommen werden, sollten die betroffenen Mitarbeiter angesichts ihres auch im Arbeitsverhältnis geltenden Persönlichkeitsrechts über den Eintrag selbst bestimmen können.[72] Dies gilt insbesondere bei Fotografien, für deren Verarbeitung bzw. Verbreitung jeder Mitarbeiter regelmäßig um seine Einwilligung gebeten werden muss. Ist den Mitarbeitern die Funktionsweise des Verzeichnisses bekannt und geben sie weitere Daten selbst freiwillig ein, so kann aufgrund der besonderen Umstände vom Vorliegen einer durch schlüssiges Verhalten erteilten Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO i.V.m. § 26 Abs. 2 BDSG ausgegangen werden.[73]

Mit Blick auf den Datenaustauch beim Betrieb eines konzernweiten Kommunikationsverzeichnisses können die beteiligten Unternehmen regelmäßig als gemeinsam für die Verarbeitung Verantwortliche für die personenbezogenen Daten angesehen werden (Art. 26 DS-GVO). Immerhin wird gemeinschaftlich das Ziel einer konzernweiten Kommunikation verfolgt und durch die Bereitstellung von Daten ein entsprechender Beitrag geleistet. Dies geschieht ferner regelmäßig über eine gemeinsam festgelegte Plattform.

3. Zentraler E-Mail-/Internet-Server

Definition:
Bei der Nutzung von Internet und E-Mail speichert und nutzt der E-Mail-/Internet-Server die ID- und Zugriffsdaten (Verkehrsdaten) aller berechtigten Benutzer sowie Daten zur Nutzungshistorie, um die Verteilung, die richtige Zuordnung und die Überprüfung der Zugriffsbefugnisse zu gewährleisten. Daneben werden auch Inhaltsdaten auf dem Server gespeichert.

Vielfach wird in Unternehmensverbünden ein gemeinsamer zentraler E-Mail-/Internet-Server eingesetzt und von einem Konzern-Service-Provider (KSP) betrieben. Dieser kann sich im Ausland, mithin auch in einem Drittland befinden.

3.1 Verhältnis Arbeitgeber und Beschäftigter

Rechtliche Grundlagen:
Im Verhältnis zwischen Arbeitgeber und Beschäftigtem ist zunächst hinsichtlich der Verarbeitung der o.g. Mitarbeiterdaten die Frage des anwendbaren Rechts zu klären. Soweit eine Privatnutzung der

72 Sog. „Employee Self Service".

73 Zur Herausforderung des Beweises schlüssiger Einwilligungserklärungen im Arbeitsverhältnis vgl. Fischer, NZA 2018, 8 (10).

betrieblichen Informations- und Kommunikationsmittel verboten ist, gilt die DS-GVO bzw. das BDSG und nicht das Telekommunikationsgesetz (TKG).[74]

Ist die Privatnutzung hingegen gestattet, so wird der Arbeitgeber nach der wohl noch herrschenden Meinung in Schrifttum und Rechtsprechung zum Anbieter von Telekommunikationsdiensten.[75] Die Ermöglichung des Internetzugangs und die E-Mail-Übertragung sind überwiegend durch die Übertragung von Signalen über Telekommunikationsnetze gekennzeichnet. Vorrangig gelten daher zunächst die Datenschutzvorschriften des TKG und nur eingeschränkt das TMG (vgl. § 11 Abs. 3 TMG). Diese bereichsspezifischen Vorschriften geben dezidiert vor, inwieweit beispielsweise Bestands- und Verkehrsdaten durch den Diensteanbieter bzw. dessen Auftragsverarbeiter überhaupt erhoben und verwendet werden dürfen.[76]

Im Verhältnis Arbeitgeber/Arbeitnehmer sind – insbesondere aus Gründen der Transparenz und zur Ermöglichung einer arbeitgeberseitigen Kontrolle – im Bedarfsfall innerbetriebliche Regelungen zum Umgang mit den Verkehrs- und Inhaltsdaten, z.B. im Rahmen einer Betriebsvereinbarung (§ 87 Satz 1 Nr. 6 BetrVG), zu treffen. Eingriffe in das Fernmeldegeheimnis durch Kontrollen des Arbeitgebers bedürfen regelmäßig der Einwilligung der Beschäftigten.[77]

3.2 Verhältnis Konzernunternehmen und Konzern-Service-Provider

Der Beschäftigtendatenschutz muss auch gewahrt bleiben, wenn der Arbeitgeber einen - ggf. konzernangehörigen - Service-Provider mit dem Betrieb der IuK-Technik beauftragt. Die Datenweitergabe an den Service-Provider bzw. der dortige Datenumgang bedürfen grundsätzlich einer Rechtsgrundlage.[78]

Geht es bei der Beauftragung des Service-Providers um reine Internet-Zugangs- oder E-Mail-Dienste, d.h. es geht im Schwerpunkt um die Telekommunikationsleistung bzw. Telemedienleistung, ist nicht von einer Verarbeitung nach den Vorschriften der DS-GVO auszugehen, da die Normen des TKG und TMG den Umgang mit den betroffenen Daten abschließend regeln und dem Dienstleister bereits entsprechende Vorgaben machen. Erst wenn ergänzende Leistungen des Providers hinzukommen, die den Umgang mit personenbezogenen Daten der verantwortlichen Stelle betreffen, so bspw. eine Speicherung und Abrufbarkeit von E-Mails, sind die Vorschriften der DS-GVO bzw. des BDSG für die Datenweitergabe und die -verwendung anwendbar.

Im Falle einer Anwendbarkeit der DS-GVO bei der Verarbeitung personenbezogener Inhaltsdaten durch den konzerninternen Service-Provider ist regelmäßig von einer weisungsgebundenen Tätigkeit auszugehen, die als Auftragsverarbeitung gem. Art. 28 DS-GVO auszugestalten ist. Gründe für die Verfolgung eigener Ziele des Konzerndienstleister sind nicht ersichtlich, da seine Pflicht in der Bereitstellung und der Administration einer Infrastruktur besteht, damit sich die Beschäftigten der Konzerngesellschaften intern oder mit Dritten per E-Mail austauschen können.[79]

4. Helpdesk

Definition:

Im Unternehmensverbund bedient man sich zur Unterstützung der technischen Infrastruktur häufig eines - ggf. dem Unternehmensverbund angehörenden - zentralen Dienstleisters (Rechenzentrum/IT-Services). Das sog. „Helpdesk“ bezeichnet einen Service zur Unterstützung der Anwender von Hard- und Software. Die Unterstützung kann per Telefon

74 Zur rechtlichen Einordnung und zur Problematik des Fernmeldegeheimnisses gem. § 88 TKG vgl. Brink/Schwab, ArbRAktuell 2018, 111.
75 Reiserer/Christ/Heinz, DStR 2018, 1501 (1507) m.w.N. **76** Ausführlich hierzu vgl. BfDI. Datenschutz und Telekommunikation (Info 5), abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO5.html.
77 Kühling/Buchner/Maschmann, BDSG § 26 Rn. 51 m.w.N.
78 Zum Konzernprivileg vgl. II., 1.
79 Vgl. Datenschutzkonferenz, Kurzpapier Nr. 13 S. 4 Anhang A am Beispiel der „Datendienste“.

oder mit Hilfe technischer Geräte sowie Software (Fernwartung) erfolgen.

Rechtliche Grundlagen:
Erfolgt die Beauftragung des Dienstleisters zur technischen Unterstützung bei der Datenverarbeitung nach konkreten Vorgaben, wird im Regelfall eine Nutzung der überlassenen Beschäftigtendaten bzw. eine Verarbeitung im Auftrag (z.B. durch die Erhebung von Protokolldaten der Nutzer) gem. Art. 28 DS-GVO vorliegen (vgl. hierzu oben unter D.).

Grundsätzlich wird der Helpdesk-Dienstleister nur tätig, um auftretende Fehler im Rahmen des Auftrags und der Weisung zu beheben. Soweit ihm hierbei Beschäftigtendaten zur Kenntnis gelangen, darf er diese nur streng zweckgebunden nutzen. Der Helpdesk-Support hat zwar im Rahmen der Fehler- und Problembehebung zwangsläufig eine bestimmte Eigenständigkeit zur Folge, diese spielt jedoch angesichts der durch den konkreten Auftrag vorgegebenen Rahmenbedingungen eine untergeordnete Rolle und umfasst insbesondere nicht die Befugnis, über die Verarbeitung und Nutzung der Daten zu anderen Zwecken zu entscheiden. Auch eine eigenständige Bestimmung über durch ihn eingesetzte Hard- oder Software vermag seine Stellung als Auftragsverarbeiter nicht zu ändern.[80] Insofern handelt es sich bei der Inanspruchnahme in der Regel um eine Datenerhebung, -verarbeitung und -nutzung im Auftrag i.S.v. Art. 28 DS-GVO und nicht um eine Verarbeitung der Daten zu eigenen Zwecken.

Eine gemeinsame Zweckverfolgung für die Verarbeitung personenbezogener Beschäftigtendaten i.S.d. Art. 26 DS-GVO wäre denkbar, wenn mit den Helpdesk-Tätigkeiten eine personenbezogene Analyse der Support-Fälle durch die datenempfangende Gesellschaft verbunden wäre, so bspw. um die Beschäftigten diesbezüglich zu schulen oder um die Qualität der Tätigkeiten insgesamt zu verbessern. In der Praxis dürfte eine aggregierte Darstellung eingegangener Helpdesk-Anfragen jedoch ausreichend sein, um bspw. vorhandene Ressourcen gezielt einzuteilen.

Soweit durch die Inanspruchnahme des Dienstleisters personenbezogene Datensätze von Mitarbeitern entstehen, die auch Leistungs- und Verhaltenskontrollen ermöglichen, bedarf es der Mitbestimmung des Betriebsrats (§ 87 Satz 1 Nr. 6 BetrVG).

5. Cloud-Computing

Definition:
Als Cloud-Computing bezeichnet man das bedarfsorientierte dynamische und skalierbare Bereitstellen einer IT-Infrastruktur über ein Netzwerk. Diese Infrastruktur kann sich dabei im zur Verfügung stellen von Rechenzeit, bis hin zum Hosting von Datenbanken oder Anwendungsprogrammen auszeichnen. In diesem Sinne wird für die Art des Dienstes eine eigene Begrifflichkeit verwendet. So existieren Lösungen wie Infrastructure as a Service (IaaS), Platform as a Service (PaaS) bzw. Software as a Service (SaaS).

Auch im Rahmen der Dienstleistungen im Unternehmensverbund kommt es häufiger zu Auslagerungen von Services in die Cloud, die eine Weitergabe von Mitarbeiterdaten und eine Verarbeitung in der Cloud beinhalten.

Rechtliche Grundlage:
Die bereits dargelegten Grundsätze für die Beurteilung einer Datenverarbeitung im Konzernverbund (vgl. C.) gelten auch uneingeschränkt für Dienstleistungen, die in der Cloud betrieben werden. Insofern fallen diese Dienste in den Bereich des Outsourcings, das grundsätzlich als Auftragsver-

80 Vgl. Art.-29-Datenschutzgruppe, WP 169 Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, angenommen am 16.02.2010, S. 17.

arbeitung, eine Verarbeitung zu eigenen Zwecken oder als eine gemeinsame Verantwortlichkeit ausgestaltet werden kann. Bedarf es auf Seiten des Dienstleisters nicht eines inhaltlichen Zugriffs auf Daten, sondern steht der technische Betrieb im Vordergrund, ist regelmäßig von einer weisungsgebundenen Tätigkeit auszugehen, die bei einem potenziellen Zugriff auf personenbezogene Daten anhand der Vorgaben des Art. 28 DS-GVO auszugestalten ist. Die Auslagerung eines Dienstes in die Cloud birgt im Übrigen Risiken für Betroffene. In diesem Zusammenhang forderten die Datenschutzbeauftragten des Bundes und der Länder im Rahmen ihrer 82. Konferenz (DSK) Anbieter von Cloud-Diensten auf, Maßnahmen anzubieten, die eine Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung gewährleisten können.[81] Ebenso haben die Artikel-29-Datenschutzgruppe[82] und der Europäische Datenschutzbeauftragte[83] in ihren Stellungnahmen Hinweise für das Einschalten eines Cloud-Dienstleisters erarbeitet.[84]

III. Personalrecruiting

Definition:
Unternehmen oder Unternehmensverbünde rekrutieren neue Mitarbeiter regelmäßig über ihre Internetpräsenz, in deren Rahmen Bewerberfragebögen online ausgefüllt und versendet werden. Auch interne Stellenbewerbungen können auf diese Weise erfolgen. Eine zentrale Stelle betreut sowohl den Stellen- als auch den Bewerberpool und leitet nach eigenständiger Vorselektion ggf. geeignete Kandidaten an andere Konzerngesellschaften weiter.

Rechtliche Grundlage:
Rechtsgrundlage für Datenverarbeitungen zum Zwecke der Durchführung des Bewerbungsverfahrens ist regelmäßig § 26 Abs. 1 Satz 1 BDSG (Erforderlichkeit zur Begründung eines Beschäftigungsverhältnisses).

Hinsichtlich der Aufbewahrung der Bewerberdaten über das Bewerbungsverfahren hinaus, zur Ermöglichung eines späteren Rückgriffs sowie zur Weiterübermittlung der Bewerberdaten an verbundene Unternehmen, bedarf es einer Einwilligung des Bewerbers. Hierbei sollte insbesondere Transparenz hinsichtlich möglicher Empfänger im Konzern einschließlich der vorgesehenen Aufbewahrungsdauer - neben den weiteren Anforderungen des Art. 13 DS-GVO hergestellt werden.[85] Das Rekrutieren über das Internet ist durch technisch-organisatorische Maßnahmen im Sinne von Art. 32 DS-GVO (Verschlüsselung etc.) zu flankieren.

Werden im Bewerbungsverfahren Bewerberdaten von einer Konzerngesellschaft an andere Konzerngesellschaften übermittelt, so insbesondere bei einem konzerneinheitlichen Bewerbermanagement, kann regelmäßig von einer gemeinsamen Verantwortlichkeit gem. Art. 26 DS-GVO ausgegangen werden. Eine alleinige Entscheidungsbefugnis über eine Einstellung, z.B. bei der Konzernmutter, würde dem nicht entgegenstehen, sollten die übrigen Gesellschaften an der Datenerhebung mitgewirkt haben.

Eine eigene Verantwortlichkeit einer Konzerngesellschaft für Bewerberdaten kommt in Fällen in Betracht, in denen eine Gesellschaft Bewerberdaten für die Besetzung eigener Vakanzen verarbeitet, ohne über einen zentralen Bewerberprozess personenbezogene Daten mit anderen Gesellschaften

81 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011, abrufbar unter https://www.lfd.niedersachsen.de/download/61458/Entschliessung_Cloud-Computing_82._DSB-Konferenz_September_2011_.pdf.
82 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf.
83 https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_de.pdf.
84 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_de.pdf.
85 Vgl. Vgl. Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Ratgeber Beschäftigtendatenschutz, S. 32.

auszutauschen.

Sollen Bewerberdaten in ein Drittland transferiert werden, ist Kapitel V der Grundverordnung zu beachten. Hat sich z.B. die in einem Drittland ansässige Konzernmutter die Einstellungsentscheidung vorbehalten, muss dieser Umstand mit den Vorgaben des. Art. 49 Abs. 1 UAbs. 1 lit. b DS-GVO in Einklang gebracht werden. Der Europäische Datenschutzausschuss führt hierzu aus, dass ein Zusammenhang zwischen der Erfüllung des Arbeitsvertrags und einer solchen Übermittlung ins Drittland im Zuge einer zentralisierten Personalabteilung im Drittland nicht bestünde.[86] Daher wird diese Ausnahme bei Personalentscheidungen mit Blick auf Bewerbungen kritisch gesehen werden müssen. Diese hindert den Verantwortlichen jedoch nicht, andere Garantien einzusetzen, so z.B. die EU-Standardvertragsklauseln oder Binding Corporate Rules.

IV. Shared-Service-Center „Human Resources"

Definition:

Im Rahmen von Shared-Services im HR-Bereich werden Dienstleistungsprozesse in einem Unternehmensverbund konsolidiert bzw. zentralisiert (z.B. die Gehaltsabrechnung oder die Personalverwaltung, Pensionskassen etc.). Dabei übernimmt eine zentralisierte Stelle (Shared-Service-Center) die Bearbeitung gleichgelagerter Prozesse aus den verschiedenen Bereichen oder Konzernunternehmen.

Rechtliche Grundlagen:

Zunächst ist zu ermitteln, ob die Weitergabe der Personaldaten an das Shared-Service-Center im Rahmen einer Auftragsverarbeitung, einer Datenübermittlung an einen Verantwortlichen oder einer gemeinsamen Verantwortlichkeit erfolgt.

Im Fall der Auftragsverarbeitung bedarf es, neben der Zulässigkeit der Datenverarbeitung insgesamt, des Abschlusses eines Vertrages mit den Mindestvorgaben des Art. 28 Abs. 3 DS-GVO.

Verfolgt die datenempfangende Konzerngesellschaft eigene Zwecke mit der Datenverarbeitung, ist die datenschutzrechtliche Zulässigkeit der Personaldatenübermittlung an das Shared-Service-Center vorrangig nach § 26 Abs. 1 Satz 1 BDSG zu beurteilen. Die Zulässigkeit der Datenweitergabe an das Shared-Service-Center kann sich im Falle eines sog. „konzerndimensionalen Arbeitsverhältnisses"[87], bei dem sich das Arbeitsverhältnis seinem Inhalt nach auch auf eine Tätigkeit für andere Konzernunternehmen oder sogar auf den gesamten Konzern erstreckt, aus § 26 Abs. 1 Satz 1 BDSG ergeben. Fehlt ein solcher Konzernbezug im Arbeitsverhältnis, müssen Datenübermittlungen an einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO gemessen werden oder können über eine Betriebsvereinbarung legitimiert werden. Hierbei kommt es jedoch wesentlich darauf an, inwieweit die jeweilige Übermittlung für die Zielerreichung als erforderlich angesehen werden kann.

Erfolgt bspw. die Erhebung von personenbezogenen Informationen zu Gehältern und Löhnen konzernweit beim Shared-Service-Center, ist diese als gemeinsam für die Verarbeitung Verantwortlicher zusammen mit den beteiligten Gesellschaften anzusehen.[88] In diesem Fall ist eine zusätzliche Vereinbarung gemäß Art. 26 DS-GVO notwendig.

Auch bei der Auslagerung der gesamten Personalabteilung an eine zentrale Konzerngesellschaft wird regelmäßig von einer gemeinsamen Verantwortlichkeit auszugehen sein, da die beteiligten Konzerngesellschaften als beteiligte örtliche Arbeitgeber zum übergeordneten Zweck der konzernweiten Personalverwaltung durch die Datenweitergaben ihren Beitrag leisten.

Befindet sich das Shared-Service-Center in ei-

86 Vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018, S.10.

87 Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Teil VI. C. I. Rn. 65 m.w.N.

88 Lezzi/Oberlin, ZD 2018, 398 (403).

nem Drittland und ist eine wirksame Betriebsvereinbarung abgeschlossen worden, kann sich der Datenimporteur im Drittland diesen Regelungen unterwerfen. Im Übrigen ist Kapitel V der Grundverordnung zu beachten. Zur Herstellung eines angemessenen Datenschutzniveaus bietet sich im Fall der Auftragsverarbeitung die Verwendung der entsprechenden EU-Standardvertragsklauseln (Controller to Processor) an. Im Falle einer Datenübermittlung kommen die zwei anderen Standardvertragsklauselwerke (Controller to Controller) der EU-Kommission in Betracht.[89] Bezüglich des alternativen Standardvertragsklauselsets ist wiederum zu beachten, dass dort ergänzende Regelungen vorgenommen werden müssen, sofern Beschäftigtendaten übermittelt werden.[90] Ferner zu beachten ist hierbei, dass die Standardvertragsklauseln die Konstellation einer gemeinsamen Verantwortlichkeit gem. Art. 26 DS-GVO nicht adäquat abdecken.

V. Zentrale Führungskräftebetreuung und -entwicklung

Definition:
Speziell in Bezug auf leitende Angestellte wird zum Teil die gesamte Personalverwaltung ausgelagert und häufig zentral bei der Holding bzw. der Konzernmutter angesiedelt.

Rechtliche Grundlagen:
Es liegt in der Natur der Sache, dass die zentrale Führungskräftebetreuung und -entwicklung durch die Holding bzw. die Konzernmutter über eine weisungsgebundene Unterstützung bei der Datenverarbeitung hinausgeht. Mithin liegt in diesen Fällen keine Auftragsverarbeitung vor, mit der Folge, dass die Weitergabe der Daten der leitenden Angestellten eine Datenübermittlung darstellt. Hierbei sind die beteiligten Konzerngesellschaften regelmäßig als gemeinsam für die Verarbeitung Verantwortliche verbunden, um den gemeinsamen Zweck der zentralen Führungskräftebetreuung zu realisieren.

Die Datenübermittlung zwischen den Konzerngesellschaften ist gem. § 26 Abs. 1 Satz 1 BDSG regelmäßig zulässig, denn die Angestelltentätigkeit ist hier in aller Regel nicht auf das jeweilige Beschäftigungsunternehmen beschränkt, sondern gerade auf die Kooperation mit der Konzernspitze angelegt. Natürlich tragen auch hier Transparenz und möglichst dezidierte arbeitsvertragliche Regelungen zur Rechtssicherheit bei.

Soweit man gleichwohl auf Art. 6 Abs. 1 lit. f DS-GVO zurückgreift, sind jedenfalls insofern keine überwiegenden Betroffeneninteressen zu erwarten, als die zentrale Führungskräftebetreuung und -entwicklung gerade Karrierechancen und Verdienstmöglichkeiten eröffnet.

VI. Übermittlung an Matrix-Vorgesetzte

Definition:
Die Matrixorganisation zählt zu den möglichen Modellen der Organisation von Stellenbeziehungen im Unternehmensverbund, nach denen Zuständigkeiten und Verantwortlichkeiten aufgebaut werden können. Im Konzernverbund wird die Fach- und ggf. auch die Personalvorgesetztenfunktion häufig auf eine oder mehrere Personen in anderen konzernangehörigen Unternehmen übertragen. Beispielsweise können Mitarbeiter den Leitern der verrichtungsbezogenen Abteilungen Beschaffung, Produktion und Absatz und gleichzeitig den objektbezogenen Produktmanagern unterstellt sein. Somit bestehen mehrere Weisungsbeziehungen, was naturgemäß auch die Übermittlung der betreffenden Personaldaten bedingt.

89 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
90 Vgl. D. II. 2.1.

Rechtliche Grundlagen:

Als Erlaubnisnorm für die Übermittlung der erforderlichen Personaldaten lässt sich zunächst § 26 Abs. 1 Satz 1 BDSG heranziehen. Ist die Matrixstruktur im Arbeitsvertrag geregelt bzw. bei dessen Abschluss für den Mitarbeiter erkennbar, so rechtfertigt die Zweckbestimmung des Arbeitsvertrages die Datenübermittlung. Auch die Aufnahme einer sog. Flexibilitätsklausel, wonach der Mitarbeiter sich bereit erklärt, in verschiedenen Konzernteilen im In- und Ausland tätig zu werden (sog. konzerndimensionales Arbeitsverhältnis), schafft hinreichende Transparenz für den Betroffenen im Hinblick auf entsprechende Datenflüsse. Soweit das Direktionsrecht des Arbeitgebers reicht, kann sich ein konzerndimensionales Arbeitsverhältnis jedenfalls auch nachträglich konkretisieren.

Im Übrigen ist die Übermittlung von Mitarbeiterdaten auch nach Vornahme einer Interessenabwägung gem. Art. 6 Abs. 1 lit. f DS-GVO zulässig, wenn diese ergibt, dass die unternehmenspolitischen und organisatorischen Interessen an der Einrichtung von Matrixstrukturen überwiegen.

Im Rahmen der Interessenabwägung ist auch zu berücksichtigen, dass die Anzahl der einem bestimmten Mitarbeiter zugewiesenen Matrixvorgesetzten begrenzt ist.

Zu prüfen ist ferner, ob durch eine vorhandene Matrixstruktur eine gemeinsame Verantwortlichkeit für die personenbezogenen Daten geschaffen wird. Dies hängt vom Zweck der jeweiligen Datenübermittlung ab. Sind bspw. zu Zwecken des Talentmanagements anderer Konzerngesellschaften und dort ansässige Vorgesetzte über sog. „Feedback-Gespräche" einbezogen, sprechen gute Gründe für eine gemeinsame Verantwortlichkeit; immerhin wirken mehrere Gesellschaften am übergeordneten Zweck der Talentförderung mit. Eine Standardisierung der Mittel der Verarbeitung personenbezogener Daten über konzernweite Vorgaben hinsichtlich der durchgeführten Gespräche würde dies entsprechend stützen.

Eine Interessenabwägung kann aber im Fall des Drittlandtransfers nur dann zu Gunsten des Unternehmens ausfallen, wenn bei dem Datenempfänger ein angemessenes Datenschutzniveau gegeben ist. War die internationale Matrixstruktur von vorneherein absehbar und ist sie damit als Bestandteil des Arbeitsverhältnisses anzusehen, können entsprechenden Übermittlungen nach Art. 49 Abs. 1 UAbs. 1 lit. b DS-GVO gestattet sein. Hierbei wird jedoch auf den jeweiligen Arbeitsvertrag und die dort geregelten Pflichten im Einzelfall abzustellen sein.[91] Ferner ist ErwG 111 zu beachten, der nur gelegentliche Übermittlungen im Rahmen der Erforderlichkeit einer Vertragserfüllung erlaubt.

VII. Remotezugriffe auf Mitarbeiterdaten

Definition:

Remotezugriffe sind Fernzugriffe, die per Wählverbindung oder Standleitung auf einen anderen Rechner erfolgen. Remotezugriffe erfolgen z.B., wenn ein auf Geschäftsreise befindlicher zugriffsberechtigter Manager mittels eines Notebooks über eine Netzwerkverbindung innerhalb seines Zuständigkeitsbereichs auf Daten seines Unternehmens zugreift.

Rechtliche Grundlagen:

Eine Definition der Übermittlung personenbezogener Daten findet sich in der Grundverordnung im Gegensatz zur alten Rechtslage[92] nicht mehr. Vielmehr wird in Art. 4 Nr. 2 DS-GVO die Verarbeitung definiert, die sich auch in einer Übermittlung personenbezogener Daten durch Offenlegung manifestieren kann.

Beim zuvor genannten Beispiel liegt keine Datenübermittlung an einen Dritten vor, wenn durch

91 Vgl. Lange/Filip in: BeckOK DatenschutzR, 25 . Ed. 2018, Art. 49 Rn. 15, die beispielsweise den Sonderfall der Mitarbeiter mit einer Zuständigkeit für Einkaufs- oder Verkaufskontakte mit Drittländern als ein Fall des Art. 49 Uabs. 1 lit. b DS-GVO ansehen.

92 Vgl. § 3 Abs. 4 Satz 2 Nr. 3 BDSG a.F.

technisch-organisatorische Maßnahmen – insbesondere die Verschlüsselung der Inhalte nach dem Stand der Technik - sichergestellt ist, dass Dritte keine Kenntnis von den Daten erhalten.

An dieser Beurteilung ändert sich nichts, wenn der Zugriff aus einem Drittland erfolgt. Entscheidend ist insoweit die organisatorische Zugehörigkeit zur verantwortlichen Stelle und nicht der (zufällige und ggf. vorübergehende) Standort. Liegt keine Übermittlung personenbezogener Daten vor, bedarf es entsprechend keiner Rechtsgrundlage für diesen Aspekt der Datenverarbeitung.

VIII. Skill-Management

Definition:
Die Personalentwicklung beinhaltet geplante Maßnahmen der Aus- und Fortbildung, der sonstigen Mitarbeiterförderung und der Organisationsentwicklung. Einen speziellen Fall bildet das sog. Skill-Management. Hierunter versteht man das Verwalten der Fähigkeiten und Qualifikationen (Skills) einzelner Mitarbeiter. Mit Hilfe konzernweit verfügbarer Skill-Datenbanken sollen die Mitarbeiter gezielt ihren Fähigkeiten entsprechend an der richtigen Stelle im Unternehmensverbund bzw. in Projektteams eingesetzt bzw. gefördert werden.

Rechtliche Grundlagen:
Neben § 26 Abs. 1 Satz 1 BDSG bei konzerndimensionalen Arbeitsverhältnissen kommt für die mit dem Aufbau konzernweiter Skill-Datenbanken verbundenen Datenübermittlungen Art. 6 Abs. 1 lit. f DS-GVO als Erlaubnisnorm in Betracht, sollte arbeitsvertraglich keine entsprechende Flexibilitätsklausel vorgesehen worden sein. Bei der Datenweitergabe ins Drittland muss zusätzlich ein angemessenes Schutzniveau gegeben sein, das anhand der Vorgaben des Kapitel V hergestellt werden kann.

Ohne die Einwilligung der betroffenen Mitarbeiter sollten keine sensitiven Daten nach Art. 9 Abs. 1 DS-GVO in Skill-Datenbanken eingegeben werden. Da Angaben über die Fähigkeiten von Mitarbeitern ohnehin eine gewisse Sensitivität aufweisen, sollten die Mitarbeiter speziell über die Funktionsweise und Zweckbestimmung einer Skill-Datenbank informiert sein. Wird den Beschäftigten die Möglichkeit eingeräumt, selbständig ihre Fähigkeiten in eine Software zur Erfassung freiwillig einzugeben, kann aufgrund der besonderen Umstände ausnahmsweise vom Vorliegen einer konkludenten Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO i.V.m. § 26 Abs. 2 Satz 3 BDSG ausgegangen werden. Zu beachten ist, dass auch die mit Einwilligung eingegebenen Skill-Daten einer Nutzungsbeschränkung im Hinblick auf das Allgemeine Gleichbehandlungsgesetz (AGG) unterliegen können.

Hinsichtlich der datenschutzrechtlichen Verantwortlichkeit für eine Skill-Datenbank bedarf es einer Prüfung ihrer Architektur im Konzern, insbesondere unter dem Gesichtspunkt, ob Beschäftigte ihre Fähigkeiten unmittelbar anderen Gesellschaften im Rahmen eines Self-Services als Verantwortliche zur Verfügung stellen oder ob der jeweilige Arbeitgeber eine solche Information in eigener Verantwortlichkeit erhebt und sodann weiterleitet. Im letzteren Fall würden gute Gründe für eine gemeinsame Verantwortlichkeit für die Daten sprechen.

Die verantwortliche Stelle hat sich beim Aufbau einer Skill-Datenbank unabhängig von den vorstehenden Ausführungen zu fragen, ob diese nicht zunächst mit pseudonymen oder anonymen Daten aufgebaut werden kann.[93] Wird eine gesuchte Fähigkeit eines Mitarbeiters über die Datenbank gefunden, kann eine Anfrage an den jeweiligen Arbeitgeber des Betroffenen über dessen Identität erfolgen.

Der Betrieb einer Skill-Datenbank bedarf der Mitbestimmung des Betriebsrats (§ 87 Abs. 1 Nr. 6 BetrVG), so dass auch entsprechende Betriebsvereinbarungen als Erlaubnisnormen in Betracht kommen, deren Regelungen im Fall des Drittlandtrans-

93 Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Datenschutzrecht, Art. 88 Rn. 179.

fers vertraglich durchgereicht werden können. Bezüglich der leitenden Angestellten sollte eine entsprechende Vereinbarung mit dem Sprecherausschuss getroffen werden.

IX. Mitarbeiterbefragung

Definition:
Mitarbeiterbefragungen sind ein Instrument zur Beschaffung von Steuerungsdaten, wobei die einzelnen Zielsetzungen unterschiedlich sein können. Vielfach geht es darum, Informationen über die Arbeitszufriedenheit, die Motivation der Mitarbeiter oder Vorgesetztenbeurteilungen abzufragen. Dies geschieht zunehmend auch online.

Rechtliche Grundlagen:
Aus datenschutzrechtlicher Sicht unbedenklich ist eine Mitarbeiterbefragung, wenn diese in anonymisierter Form, d.h. ohne Möglichkeit eines Rückschlusses auf bestimmte Mitarbeiter sowie auf Grundlage einer informierten und freiwilligen Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO i.V.m. § 26 Abs. 2 BDSG erfolgt. Der Hinweis auf die Freiwilligkeit sollte in den Fragebogen - optisch hervorgehoben - aufgenommen werden.[94]

Die Weitergabe von personenbezogenen Arbeitnehmerdaten an einen externen Dienstleister zur Auswertung der Antworten ist anhand der allgemeinen Abgrenzungskriterien zu beurteilen. Bei der Mitarbeiterbefragung besteht bezüglich der Abgrenzung zwischen Übermittlung und Auftragsverarbeitung die Schwierigkeit, dass eine Mitarbeiterbefragung grundsätzlich über Weisungen vorgegeben werden kann, Teile der Dienstleister jedoch einen Vertrag zur Auftragsverarbeitung ablehnen. Grund hierfür sei, dass ansonsten der Auftraggeber per Weisung und damit nach seinem Ermessen die Herausgabe von personenbezogenen Daten verlangen könne. Dem stünde das Wesen einer anonymen Mitarbeiterbefragung entgegen.

Je nach Ausgestaltung als Auftragsverarbeitung oder Übermittlung an einen Verantwortlichen sollten in einem Datenschutzvertrag zumindest die verschiedenen Rollen der Beteiligten hinsichtlich der Erfüllung von Betroffenenrechten ebenso dargestellt werden wie die vorgesehenen Zwecke bei der Datenauswertung sowie angemessene technisch-organisatorische Maßnahmen.

Sollte eine Mitarbeiterbefragung durch den Konzern selbst organisiert sein, ist eine gemeinsame Verantwortlichkeit für solche Fälle naheliegend, in denen es eine Befragung des gesamten Konzerns gibt und hierzu personenbezogene Daten der Beschäftigten zwecks der Ansprache per E-Mail an einer Stelle zentral verarbeitet werden.

Aus Gründen der Akzeptanz empfehlenswert und ggf. betriebsverfassungsrechtlich notwendig (zu Personalfragebögen bzw. Beurteilungsgrundsätzen siehe § 94 BetrVG) ist die Beteiligung der Mitarbeitervertretung.[95]

Wird eine unter § 94 BetrVG fallende Befragungsaktion von der ausländischen Konzernspitze per E-Mail durchgeführt, so ändert dies nichts an der notwendigen Mitbestimmung.[96]

X. Compliance

Definition:
Der Begriff Compliance beinhaltet die Einhaltung von Gesetzen und Richtlinien sowie von freiwilligen Kodizes (Selbstverpflichtungen) in Unternehmen.

Im Rahmen der Erfüllung allgemeiner Compliance-Vorgaben (z.B. Sarbanes Oxley Act, Corporate Governance Codex) entstehen unternehmensübergreifende Reportingstrukturen, über welche personenbezogene Informationen über die Verletzung gesetzlicher oder betrieblicher Vorgaben erfasst,

94 Vgl. auch BfDI, 20. Tätigkeitsbericht - 2003/2004, 120 = RDV 2004, 187.

95 Zur Mitbestimmung des (Konzern-)Betriebsrats bei elektronischer Mitarbeiterbefragung vgl. BAG, Beschluss vom 11.12.2018, 1 ABR 13/17 sowie BAG, Beschluss vom 21.11.2017 - 1 ABR 47/16.

96 Vgl. Hess. LAG, BB 2001, 2432 sowie Däubler, Gläserne Belegschaften?, 4. Aufl., Rn. 838.

unter Beteiligung der Konzernrevisions- und / oder Konzernsicherheitsabteilung zentral aufgeklärt und zentralen Entscheidungsstellen (Compliance Officer, Clearing Committee, Konzernvorstand) zugeleitet werden.

Rechtliche Grundlagen:
Als rechtliche Grundlagen kommen § 26 Abs. 1 Satz 1 BDSG und Art. 6 Abs. 1 lit. f DS-GVO in Betracht. Die Übermittlung relevanter personenbezogener Beschäftigtendaten zwischen Konzerngesellschaften kann u.U. auf die Zweckbestimmung des Arbeitsverhältnisses gestützt werden (§ 26 Abs. 1 Satz 1 BDSG). Voraussetzung ist aber zumindest, dass das Arbeitsverhältnis durch eine entsprechende, für den Mitarbeiter transparente betriebliche Organisation und eine eindeutige Funktionszuweisung im Konzern mitgestaltet wird.

Für Beschäftigungsverhältnisse, die bereits vor der organisatorischen Einrichtung der entsprechenden zentralen Funktionen und Reportingstrukturen entstanden sind, so dass eine entsprechende Ausgestaltung bzw. Einbeziehung in das Arbeitsverhältnis fraglich ist, kann ersatzweise auf Art. 6 Abs. 1 lit. f DS-GVO zurückgegriffen werden. Das betriebliche Interesse an der Einhaltung von Compliance-Vorgaben überwiegt grundsätzlich das Interesse des Betroffenen am Ausschluss entsprechender Datenübermittlungen. Allerdings müssen die zur Erfüllung der Compliance-Anforderungen eingesetzten Systeme (Videoüberwachung, Whistleblowing-Systeme) stets am Prinzip der Verhältnismäßigkeit ausgerichtet werden. Insofern kommt es bei der Beurteilung von Whistleblowing-systemen beispielsweise auch auf die Art der personenbezogenen Daten an, die über die jeweilige Hotline gemeldet werden sollen.[97] Bei Whisteblowing-Systemen kommt im Übrigen auch eine Rechtfertigung nach Art. 6 Abs. 1 lit. c DS-GVO in Betracht, sollte es eine rechtliche Verpflichtung aus dem Unionsrecht oder einer mitgliedstaatlichen Norm geben.[98] Im Zuge derAufklärung von Straftaten im Beschäftigungsverhältnis ist ein Rückgriff auf § 26 Abs. 1 Satz 2 BDSG möglich.

Im Konzernumfeld wir die Compliance regelmäßig gesellschaftsübergreifend gesteuert, indem beispielsweise lokale Vorfälle, die einer Untersuchung bedürfen, in einer Software mit Zugriffsrechten anderer Konzerngesellschaften dokumentiert werden. Ferner ist denkbar, dass ein vorhandener Betriebsrat oder der Datenschutzbeauftragte in Ermittlungen zur Compliance einbezogen werden. Neben der Frage der erforderlichen Zugriffsrechte auf personenbezogene Daten einer Compliance-Untersuchung bedürfen die datenschutzrechtlichen Verantwortlichkeiten einer besonderen Begutachtung. Bei einer konzernübergreifenden Compliance-Maßnahmen sprechen gute Gründe für eine gemeinsame Verantwortlichkeit, sollten die lokalen Gesellschaften personenbezogene Daten der Beschäftigten den anderen Gesellschaften für die Aufklärung eines Sachverhaltes zur Verfügung stellen. Es dürfte jedoch genauso möglich sein, eine alleinige Verantwortlichkeit einer Gesellschaft zu begründen, insbesondere wenn eine Einbeziehung anderer Konzerngesellschaften nicht erfolgt und Compliance-Fälle lediglich in anonymisierter Form bspw. an eine Konzernmutter berichtet werden.

XI. Bonusprogramme

Definition:
Bonusprogramme sollen die Mitarbeitermotivation fördern, indem den Mitarbeitern die Möglichkeit geboten wird, an einer positiven Unternehmensperformance, zu der sie beigetragen haben, zu partizipieren. Ein Beispiel hierfür sind sog. Aktienoptionspläne, bei denen den teilnehmenden Mitarbeitern im Rahmen einer aktienbasierten Vergütung die Option eingeräumt wird, eine bestimmte Anzahl von

97 Vgl. Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz, S. 5.
98 Z.B. gem. § 25a Abs. 1 Satz 6 Nr. 3 KWG.

Unternehmensaktien zu einem bestimmten Zeitpunkt gratis bzw. verbilligt zu erwerben.

Rechtliche Grundlagen:
Bonusprogramme werden in der Regel einvernehmlich entweder auf Grundlage arbeitsvertraglicher Regelung oder - z.B. bei nachträglicher Einführung - auf Basis einer freiwilligen Einwilligung des Mitarbeiters durchgeführt. Als Rechtsgrundlagen für die erforderliche Personaldatenverarbeitung kommt mithin Art. 6 Abs. 1 lit. a DS-GVO i.V.m. § 26 Abs. 2 BDSG in Betracht.

Die Übertragung der Abwicklung des Prämiensystems an einen externen Dienstleister kann im Übrigen im Wege einer Auftragsverarbeitung gem. Art. 28 DS-GVO erfolgen.

Im Fall von konzerndimensionalen Arbeitsverhältnissen, bei denen die Gewährung bestimmter Boni vertraglich fixiert worden ist, kann Art. 49 Abs. 1 UAbs. 1 lit. b DS-GVO die Rechtsgrundlage für die Übermittlung der erforderlichen Mitarbeiterdaten an ein konzernangehöriges Unternehmen im Drittland darstellen. Eine von vornherein feststehende Weiterübermittlung an einen im Drittland niedergelassenen Dienstleister zwecks Verwaltung der Aktienoptionspläne ist entweder auf Basis einer entsprechenden Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO i.V.m. § 26 Abs. 2 BDSG i.V.m. Art. 49 Abs. 1 UAbs. 1 lit. a DS-GVO oder gem. Art. 49 Abs. 1 UAbs. 1 lit. c DS-GVO grundsätzlich für Einzelfälle möglich. Der Europäische Datenschutzausschuss hat diesbezüglich jedoch Bedenken geäußert, die Beauftragung eines im Drittland niedergelassenen Dienstleisters für das Gehaltszahlungsmanagement als einen Vertragsschluss im Interesse des Betroffenen zu qualifizieren.[99] Hinsichtlich der Stock Options dürfte sich die Problematik in der Praxis insofern nicht stellen, als die Durchführung der Aktienoptionspläne auf Basis einer informierten Einwilligung der Mitarbeiter erfolgt. Für die Wirksamkeit der Einwilligungserklärungen von Mitarbeitern im Zusammenhang mit Bonusprogrammen spricht, dass den Betroffenen nur die Gelegenheit zur Wahrnehmung einer Vergünstigung geboten wird (vgl. § 26 Abs. 2 Satz 2 BDSG).

XII. Unternehmenstransaktionen

Definition:
Konzernstrukturen unterliegen vielfach einem ständigen Wandel, sei es, dass der Konzern neue Unternehmen erwirbt, oder dass bisherige Konzernunternehmen veräußert oder umstrukturiert werden. Vor diesem Hintergrund stellt sich die Frage, wie der Mitarbeiterdatenschutz bei den entsprechenden Unternehmenstransaktionen gewährleistet werden kann.

Rechtliche Grundlagen:
Im Rahmen von Unternehmenstransaktionen finden sog. Due-Diligence-Prüfungen statt. Potenzielle Erwerber benötigen zu ihrer Meinungsbildung ggf. auch personenbezogene Informationen der Mitarbeiter des zu erwerbenden Unternehmens. Als Rechtsgrundlage für die hiermit verbundene Übermittlung der Mitarbeiterdaten an den potenziellen Erwerberkommt entweder die Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO[100] i.V.m. § 26 Abs. 2 BDSG oder die Interessenabwägung gem. Art. 6 Abs. 1 lit. f i.V.m. Abs. 4 DS-GVO in Betracht. Die Erforderlichkeit der Datenübermittlung lässt sich aus der Erfüllung arbeitsvertraglicher Pflichten nur schwerlich herleiten.

Abzuwägen ist insoweit das Interesse an der Realisierung der etwaigen Unternehmenstransaktion mit den Vertraulichkeitsinteressen der Mitarbeiter. Hierbei sind die zu übermittelnden Datenkategorien ebenso von Relevanz wie der Umfang der Daten.

99 Vgl. Europäischer Datenschutzausschuss, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, Ziff. 2.3.

100 Zu den Besonderheiten der Einwilligung im Bereich der „Asset Deals“ vgl. Hansen-Oest, DSB 2020, 60 (61).

Bei besonderen Kategorien sind die Einschränkungen des Art. 9 DS-GVO zu beachten, der eine Verarbeitung besonderer Kategorien personenbezogener Daten nur in den Fällen des Absatzes 2 zulässt (zur Weitergabe sensitiver Mitarbeiterdaten vgl. Ziff. II. 2.). Im Bereich der Unternehmenstranskationen dürfte regelmäßig lediglich die Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO i.V.m. 26 Abs. 2 u. 3 BDSG in Frage kommen.

Hinsichtlich der datenschutzrechtlichen Verantwortlichkeiten ist es bei der Übermittlung personenbezogener Daten in der Due-Diligence-Phase naheliegend, die beteiligten Stellen als gemeinsam für die Verarbeitung einzustufen. Beide Stellen sind durch den gemeinsamen Zweck der Ermöglichung und Abwicklung einer Diligence-Prüfung miteinander verbunden und einigen sich hierbei regelmäßig auf eine gemeinsame Plattform zum Datenaustausch („Data-Room")[101] Wird ein externer Dienstleister für den Betrieb eines Data-Rooms eingeschaltet, besteht die Pflicht, mit diesem einen Vertrag zur Auftragsverarbeitung abzuschließen.

Jede Übermittlung ist auf die zum gegebenen Zeitpunkt unbedingt erforderlichen Daten zu beschränken.[102] Auch auf die Sicherheit der übermittelten Daten ist zu achten und es ist dafür Sorge zu tragen, dass Daten z.B. strikt im besonders abgesicherten sog. „Data-Room" gehalten werden. Nach Möglichkeit sollten lediglich anonymisierte oder statistisch aufbereitete, aggregierte Daten weitergegeben werden.

101 Vgl. auch Bach, EuZW 2020, 175 (176), der auf die weite Auslegung einer datenschutzrechtlichen Verantwortlichkeit verweist.
102 Vgl. Simitis/Hornung/Spiecker gen. Döhmann/Schantz DSGVO Art. 6 Rn. 128.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Ansprechpartner: RA Steffen Weiß, LL.M.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 228 96 96 75-00
Fax: +49 228 96 96 75-25
www.gdd.de
info@gdd.de

Stand:
Version 1.0 (Juni 2020)