Datenschutzrechtliche Rahmenbedingungen

für den Einsatz von „Workday“ bei Sanofi-Aventis Deutschland GmbH

Rechtsgutachten

erstattet im Auftrag des Unternehmenssprecherausschusses

von

Prof. Dr. Wolfgang Däubler, Bremen

Inhaltsverzeichnis

A. Sachverhalt

Die weltweit tätige Sanofi-Aventis Groupe hat sich entschlossen, sich im Bereich der Personaldatenverarbeitung der Hilfe der Firma Workday zu bedienen. Diese hat ihre Konzernspitze in den USA, verfügt jedoch auch über eine rechtlich selbständige Niederlassung in Dublin.

I. Das Master Subscription Agreement (MSA) samt Anhängen

Am 11. Oktober 2013 wurde zwischen der Sanofi-Aventis Groupe und Workday ein „Master Subscription Agreement“ (MSA) geschlossen das die Zusammenarbeit zwischen den Vertragsparteien detailliert regelt. Obwohl es auf Englisch abgefasst ist, unterliegt das MSA nach seiner Ziffer 10.8 ausschließlich französischem Recht; als Gerichtsstand ist Paris vereinbart.

Die Einschaltung von Unterauftragnehmern ist in Ziffer 10.7 des MSA geregelt. Die bei Vertragsabschluss vorhandenen Unterauftragnehmer werden Sanofi-Aventis in Form einer Liste benannt. Die Einschaltung neuer Unterauftragnehmer wird schriftlich mitgeteilt. Hat Sanofi-Aventis gegen sie unter Berücksichtigung der Grundsätze von Treu und Glauben Bedenken, muss es diese unverzüglich unter Nennung der Gründe („in reasonable detail“) Workday mitteilen. Anschließend findet eine Diskussion zwischen beiden Vertragspartnern statt. Eine Einschaltung des Unterauftragnehmers ist nur mit schriftlicher Zustimmung von Sanofi-Aventis möglich, die aber nicht ohne ausreichenden Grund („unreasonably“) verweigert oder verzögert werden darf.

Was Fragen der Datenverarbeitung angeht, so verweist Ziffer 5.3 des MSA auf die einschlägige Anlage A („Data Processing Exhibit“). Hier findet sich im Definitionsteil eine Abgrenzung des Unterauftragnehmers; erfasst sich lediglich Unternehmen, die nicht zum Workday-Konzern gehören. Um Zweifel auszuschließen, wird ein Rechenzentrum nicht zu den Unterauftragnehmern gezählt. Die inhaltlichen Voraussetzungen ihrer Einschaltung sind in Ziffer 9 des Exhibits geregelt. Dort ist festgelegt, dass Unterauftragnehmer nur für beschränkte Aufgaben („limited services“) eingeschaltet werden dürfen. Workday wird dafür sorgen, dass der Unterauftragnehmer die personenbezogenen Daten nicht für andere Zwecke verwendet als die mit Workday

vereinbarten. Workday verlangt außerdem eine schriftliche Vereinbarung, wonach der Unterauftragnehmer Bedingungen befolgen wird, die nicht weniger Schutz als der vorliegende Anhang gewähren. Workday wird jeden Unterauftragnehmer namhaft machen und wird allen seinen Kunden eine Zusammenfassung der Bedingungen übermitteln, unter denen Daten verarbeitet werden. Workday ist überdies für alle Handlungen und Unterlassungen des Unterauftragnehmers haftbar, wie wenn sie von ihm selbst stammen würden.

Die Frage, was geschieht, wenn der Unterauftragnehmer seinerseits eine Drittfirma einschaltet („Unter-Unterauftragnehmer"), wird nicht ausdrücklich angesprochen.

Ein besonderer Abschnitt ist der Datenübermittlung in die USA gewidmet. Nach Ziffer 5.1 des Exhibits garantiert Workday, dass in den USA angesiedelte Konzerngesellschaften die bestehende Safe-Harbor-Zertifizierung beibehalten, solange die Safe-Harbor-Grundsätze durch die EU als legitime Basis für die Übermittlung von Daten in die USA anerkannt werden.

Nach Ziffer 5.3 des Exhibits werden die Daten von Workday in Rechenzentren gespeichert, die im Europäischen Wirtschaftsraum (EWR) gelegen sind. In Übereinstimmung mit dem MSA und dem vorliegenden Exhibit ist ein Zugriff auf diese Daten von Drittländern aus nur möglich, wenn es sich um die USA oder ein Land handelt, dessen Datenschutzniveau von der EU-Kommission als angemessen anerkannt ist. Der Zugriff darf nur für Zwecke erfolgen, die im MSA niedergelegt sind; eingeschlossen ist dabei das Update geleisteter Dienste und die Verhinderung oder Bewältigung von auftauchenden technischen und anderen Problemen.

Die Frage des Zugriffs durch hoheitliche Stellen in dem jeweiligen Land ist in Ziffer 7.2 des Exhibits angesprochen. Danach wird ein solcher Zugriff dem Kunden unverzüglich mitgeteilt, sofern dies nicht durch das anwendbare Gesetz verboten ist. Dies spricht inhaltlich insbesondere Regelungen des US-Patriot Act an, die im (weit verstandenen) Rahmen der Terrorismusbekämpfung umfassende staatliche Zugriffsrechte gewähren und dies mit der Besonderheit, dass effektiv erfolgte Zugriffe geheim gehalten werden müssen. Zwar unterliegt das Exhibit nach seiner Ziffer 13.2 genau wie das MSA dem französischen Recht, doch handelt es sich bei dem Patriot Act um eine sog. Eingriffsnorm,

die auch dann verbindlich ist, wenn im Übrigen US-Recht auf eine Vertragsbeziehung keine Anwendung findet.

II. Das Datenschutzabkommen zwischen Sanofi-Aventis Deutschland GmbH und der Sanofi-Aventis Groupe Paris

Zwischen der Sanofi-Aventis Deutschland GmbH (abgekürzt: SADG) und der Konzernspitze, der Sanofi-Aventis Groupe mit Sitz in Paris (abgekürzt: SAG) existiert ein (undatiertes) Datenschutzabkommen („Data Processing Agreement"), das durch den zweiten Änderungsvertrag vom 30. Januar 2015 an die Situation angepasst wurde, die durch die Einschaltung von Workday entstanden ist.

Unter Ziff. 2 bezeichnet sich das Abkommen als „Rahmenabkommen", in dem SADG die SAG ermächtigt, personenbezogene Daten durch Anwendung bestimmter IT-Applikationen zu verarbeiten. Der rechtliche Rahmen für diese Verarbeitung im Namen von SADG besteht nach Ziffer 3 Absatz 1 aus dem Abkommen und seinen Anhängen, den schriftlichen Anweisungen von SADG und den bindenden konzerneinheitlichen Richtlinien („binding corporate rules").

Nach Ziffer 3 Absatz 2 wird SAG die Zweckbindung der Daten beachten, die im Einzelnen in den Anlagen beschrieben ist.

SADG erhebt, verarbeitet und übermittelt personenbezogene Daten in Übereinstimmung mit dem BDSG; sollte dieses in bestimmter Hinsicht auch von SAG zu beachten sein, wird dies von SADG an SAG unter Wahrung einer angemessenen Frist mitgeteilt. Nach Ziff. 4 Buchstabe e ist es die alleinige Verantwortung von SADG, Fragen von Betroffenen, des Betriebsrats, des Unternehmenssprecherausschusses, der Aufsichtsbehörde für den Datenschutz sowie des betrieblichen Datenschutzbeauftragten zu beantworten.

SAG verarbeitet nach Ziffer 5 Buchstabe a die personenbezogenen Daten in Übereinstimmung mit dem Abkommen und seinen Anhängen sowie den Anweisungen

von SADG nach französischem Datenschutzrecht. Auch für SAG gilt der Grundsatz, dass eine Verarbeitung nur für Zwecke zulässig ist, die in den Anhängen beschrieben sind.

Eine Übermittlung von Daten in Drittländer außerhalb der EU ist nur zulässig, wenn SADG schriftlich von einem entsprechenden Vorhaben in Kenntnis gesetzt wurde und schriftlich zustimmte, wobei die Zustimmung nicht ohne sachlichen Grund verweigert werden darf. SAG wird dafür sorgen, dass der eingeschaltete Dritte die Vertraulichkeit und Sicherheit der personenbezogenen Daten wahrt und sie strikt nur nach Weisung verarbeitet. Dies gilt allerdings nicht für Personen, die durch Gesetz ermächtigt oder verpflichtet sind, Zugriff auf die Daten zu nehmen. Darunter würde – so muss man schließen – auch ein Zugriff nach dem US Patriot Act fallen. Dass gesetzliche Verpflichtungen den vertraglichen Abreden vorgehen, wird auch in Ziffer 7 Buchstabe a deutlich („unless legally required“).

Bei Auskunftsersuchen von Betroffenen und dem Betriebsrat von SADG arbeiten die Vertragsparteien nach Treu und Glauben zusammen. Die Verantwortung für die Erteilung der Auskunft liegt bei SADG.

Die in den Anhängen des ursprünglichen Vertrags beschriebenen Verwendungszwecke sind aufgrund der Neufassung durch die Änderungsvereinbarung vom 30. Januar 2015 weitestgehend überholt und sollen deshalb hier nicht wiedergegeben werden.

Die Änderungsvereinbarung definiert in ihrem Anhang 1 Nr. 2 die Zwecke der Datenverarbeitung, die den Personalabteilungen (HR) zur Verfügung stehen. Unter der Überschrift „Global Human Resources Management (Workday)“ wird unter „Scope, Type and Aim of Process“ ausgeführt:

„Administration of employee data for local, global processes and of the organizational structure.
Implementation of operational regulations (e. g. Compensation, Personnel data Management, Performance Management, succession planning).
Maintenance and administration of individual people development and succession planning.
Reporting functions to global matrix organisations.”

Als Unterauftragnehmer findet Workday Erwähnung. Server stehen in Dublin und Amsterdam. Zu den Zugriffsberechtigten gehören auch ca. 15 globale Administratoren.

III. Die verbindlichen Unternehmensregelungen zum Datenschutz

Bei der Übermittlung von Daten in Länder ohne angemessenes Datenschutzniveau müssen die Schutzdefizite durch vertragliche Abmachungen ausgeglichen werden. Möglich ist, einen der Musterverträge der EU-Kommission zugrunde zu legen, was eine Genehmigung durch die Aufsichtsbehörde für den Datenschutz überflüssig macht. Zweite Möglichkeit ist die Vereinbarung von verbindlichen Verhaltensregeln („binding corporate rules"), was nur bei Konzernen und bei kooperierenden Unternehmen in Betracht kommt.

Die Sanofi-Aventis-Gruppe besitzt seit einer Reihe von Jahren bindende Verhaltensregeln zur Übermittlung von personenbezogenen Daten („Sanofi-Aventis Group in-house rules on the transfer of personal data"). Der Sinn der Regelung wird nach ihrem Abschnitt I insbesondere darin gesehen, ein einheitliches Datenschutzniveau für alle Standorte von Sanofi-Aventis weltweit zu schaffen, also insbesondere auch Regeln für die Übermittlung in Länder ohne angemessenes Datenschutzniveau aufzustellen. Werden Daten von einem Land in ein anderes übermittelt, so soll nach Abschnitt II das jeweils höhere gesetzliche Datenschutzniveau maßgebend sein. Dabei werden als Mindeststandard die Wahrung des Grundsatzes von Treu und Glauben bei Erhebung, Übermittlung und Verarbeitung vorgesehen. Außerdem dürfen personenbezogene Daten nur für bestimmte, ausdrücklich benannte and legitime Zwecke erhoben, übermittelt und verarbeitet werden; die Weiterverarbeitung darf nicht unvereinbar mit dem ursprünglichen Zweck sein. Die personenbezogenen Daten müssen präzise, nicht unvollständig und dem Zweck angemessen sein. Ist dies nicht der Fall, müssen sie berichtigt, ergänzt, gelöscht oder gesperrt werden. Die personenbezogenen Daten dürfen nicht länger gespeichert bleiben, als es für die Verarbeitung und die Übermittlung erforderlich ist. Auch ist die Datensicherung zu gewährleisten.

Die englische Originalversion dieser Festlegungen lautet:

- to collect, transfer and process the personal data fairly,
- to collect, transfer and process the personal data for determined, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
- to collect, transfer and process personal data that are accurate, suitable, relevant and not excessive for the purposes of the transfer and processing, consequently, inaccurate or incomplete data must be rectified, supplemented, erased or their further processing must be suspended,
- not to keep the personal data beyond the length of time needed for processing and transfer,
- to adopt suitable means of security…"

Im Folgenden wird betont, Datenverarbeitung und Datenübermittlung müssten eine rechtliche Grundlage haben. Als solche werden genannt:

„- the data subject has given his consent; or
- the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- the processing is necessary for compliance with a legal obligation to which the group is subject; or
- the processing is necessary to save the vital interest of the data subject; or
- the processing is necessary for the performance of a task carried out in the public interest or in the interest of a third party to whom the data are disclosed; or
- the processing is necessary for the purpose of legitimate interests pursued by the controller except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."

Soweit sensitive Daten übermittelt werden, muss ihre Verarbeitung auf einer der folgenden Grundlagen beruhen:

„- The explicit consent of the data subject; or
- The necessity for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

- The processing relates to sensitive data which are manifestly made public by the data subject; or
- The processing of sensitive data is necessary for the establishment, exercise or defence of legal claims; or
- The processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those sensitive data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy, or
- The processing of the sensitive data is required for reasons of substantial public interest laid down either by national law or decision of the supervisory authority."

Niederlassungen, die in eine Datenübermittlung einbezogen sind, müssen alle geeigneten Schritte unternehmen, um für die Einhaltung dieser Grundsätze zu sorgen; dazu gehören auch die Standardverträge der EU. Die im Europäischen Wirtschaftsraum ansässigen Niederlassungen müssen sicher stellen, dass die Betroffenen von der Datenübermittlung informiert werden und dass sie ihre Rechte auf Auskunft, Berichtigung und Sperrung geltend machen können.

Um die Beachtung der verbindlichen Unternehmensregeln sicher zu stellen, sieht ihr Abschnitt IV eine Reihe von Maßnahmen vor. Das zählt ein jährliches Datenschutz-Audit, aber auch ein Beschwerdeverfahren, in dem insbesondere Verstöße gegen die verbindlichen Unternehmensregelungen geahndet werden. Dabei richten sich Ansprüche gegen die in der EU ansässigen Unternehmen, die ggf. auch beweisen müssen, dass sie bei einer Übermittlung in einen Drittstaat alle angemessenen Schutzmaßnahmen getroffen haben.

Anhang IV beschreibt die Beschäftigtendaten und die Zwecke, für die sie verwendet werden dürfen. Dabei geht es um Personaleinsatz und Personalentwicklung auf internationaler Ebene. Deshalb ist bei folgenden Daten nach den Grundsätzen der verbindlichen Unternehmensregeln zu verfahren:

„- organization, particularly controlling access to the Group´s IT systems, technical

traceability and administrative workflow monitoring systems, as well as Group electronic directories,
- salary adjustments (annual increases, flexible pay, other pay-related information),
- international mobility,
- human resource development, particularly skills, training and individual and professional development plans,
- staff administrative management such as travel allowance, expenses, etc."

In Übereinstimmung mit dem jeweiligen nationalen Recht besteht bei bestimmten Daten eine hohe Wahrscheinlichkeit der Übermittlung: Vor- und Zuname, Privatadresse, IT Identifizierung, berufliche E-Mail-Adresse, Arbeitsort, (zuständiger) Manager, Gehalt, Beförderungen, Informationen zu flexiblen Entgeltbestandteilen, Inhalt des Arbeitsvertrags, individuelles Profil, individuelle Ziele, fachliche Fähigkeiten, Berichte über Weiterbildungsmaßnahmen, Zeiteinteilung, Sozialleistungen, Mobilität und Beförderungsvoraussetzungen, Plan für Karriereentwicklung und jede beförderungsrelevante Information. Einbezogen kann auch eine Liste mit absolvierten Arbeiten sein, über Arbeitszeit und Gegenstände, die ihm anvertraut wurden. Auch die Namen von Autoren und Mitverfassern von Dokumenten werden erfasst, ebenso wie die Buchungskontrolle und die elektronischen Unterschriften, die im Rahmen der Gesundheitsversorgung erforderlich sind.

IV. Gesamtbetriebsvereinbarung zum Personalinformationssystem Workday

Zwischen dem Gesamtbetriebsrat der Sanofi-Aventis Deutschland GmbH (SADG) und der Geschäftsführung der SADG wurde eine vorläufige Vereinbarung über den Einsatz von Workday geschlossen. Die am 29. 1. 2015 zustande gekommene „Gesamtbetriebsvereinbarung zum Personalinformationssystem Workday" soll so lange gelten, bis eine finale Fassung von beiden Seiten unterzeichnet ist. Unter Ziffer 4 der vorläufigen Gesamtbetriebsvereinbarung ist festgelegt, dass sich die für Sanofi eingesetzten workday-Server ausschließlich innerhalb der EU, d. h. in Dublin und in Amsterdam befinden und dass sie nur dort betrieben, gehostet und gewartet werden. Ein

Zugriff zwecks Hosting und Support darf ausschließlich durch Mitarbeiter der Firma Workday erfolgen, die in der EU angesiedelt sind.

Eingehend wird unter Ziffer 5 festgelegt, welche Funktionalitäten des Personalinformationssystems Workday ausschließlich genutzt werden dürfen. Dazu heißt es:

- Personaldatenpflege

  - Administration der Mitarbeiterdaten für zentrale Prozesse sowie Organisationsstruktur
  - Prozesse: Pflege Mitarbeiterdaten, Tätigkeits- und Vergütungsveränderungen, Versetzungen/Delegationen, Vertragsänderungen, Arbeitszeitänderungen, Management von Freistellungen außerhalb des Katalogs für kurzfristige Freistellungen gemäß § 8 MTV Chemie (z. B. Elternzeit, Mutterschutz, bezahlte Freistellung) sowie die Abwesenheit Urlaub für außertarifliche Angestellte.

- Leistung und Vergütung (Performance & Recognition)

  - Dokumentation des gesamten Performancemanagementprozesses. Hierzu zählen insbesondere die jährlich vereinbarten Mitarbeiterprioritäten und Kompetenzen, die Zielerreichungsgespräche sowie die Zielerreichungsgrade. Die Parteien sind sich einig, dass die Gespräche zwischen Vorgesetztem und Mitarbeiter zur Vereinbarung und Änderung von Prioritäten, Zielen oder Kompetenzen sowie das Jahresendgespräch zur Erreichung der getroffenen Vereinbarung durch die Nutzung von Workday nicht beeinträchtigt werden oder gar entfallen dürfen.

- Talentförderung und Nachfolgeplanung (Talent Management & Succession Planning)

  - Ziel und Zwecksetzung ist die Dokumentation und Unterstützung der Umsetzung von Maßnahmen der zielgerichteten, langfristigen und strategischen Förderung und Entwicklung von Mitarbeitern mit einem globalen, ganzheitlichen Ansatz. Der Talent Development Prozess umfasst Strategien, Methoden und Maßnahmen, mit denen das Unternehmen sicherstellt, dass die für den Geschäftserfolg wichtigen Positionen dauerhaft mit den geeignete Mitarbeitern besetzt sind. Talent Management bezieht sich auf die Identifikation, Gewinnung, Bindung und Förderung von Mitarbeitern.

- Online-Prozess Talent Development beinhaltet den Talent Review sowie die Unterstützung der Nachfolgeplanung sowie Personalentwicklung, lokal und global.

- Der Prozess Talent Review wird über Workday abgebildet. Dieser beinhaltet für Tarifmitarbeiter die Dokumentation des Gesprächs zwischen Mitarbeiter und Vorgesetztem über Entwicklungsmöglichkeiten. Für AT-Mitarbeiter gilt der Full Talent Review, der zusätzlich zum Talent Review eine Potentialeinschätzung enthält.

- Hierzu werden Mitarbeiterdaten für unterschiedliche HR-Prozesse (Bewertungen, Mobilität, Informationen zum Lebenslauf) zur Verfügung gestellt.

- Der Talent Management – Prozess wird unterstützt durch die Abteilung Personalentwicklung, Informationen zum Lebenslauf, Berufserfahrung, Tätigkeitsinteressen, können vom Mitarbeiter selbst und freiwillig erstellt werden. Die Parteien sind sich einig, dass mit dem elektronischen Lebenslauf keine Leistungs- oder Verhaltenskontrollen durchgeführt werden. Darin enthaltene personenbezogene Daten dürfen nicht arbeitsrechtlich verwertet werden. Ebenso bleibt es ohne arbeitsrechtliche Konsequenz, wenn ein Mitarbeiter freiwillige Eingaben nicht tätigt. Auch ohne freiwillige Angaben nimmt der Mitarbeiter an der Talentförderung und Nachfolgeplanung teil.

- Die Mitarbeiter können Daten, die sie in einem Profil des sozialen Netzwerks LinkedIn erstellt haben (zum Beispiel Berufserfahrung, Kenntnisse etc.), im Wege des Datendownloads importieren. Hierzu muss sich der Mitarbeiter zunächst mit seinem Benutzernamen und Passwort bei LinkedIn anmelden. Das Passwort wird in Workday nicht gespeichert. Dem Mitarbeiter werden sodann die Angaben aus LinkedIn angezeigt und er kann auswählen, ob und ggf. welche Daten er in sein Workday-Profil übernehmen möchte. Sofern der Mitarbeiter Daten übernimmt, werden diese im Rahmen des Talent Management- und Nachfolgeplanungsprozesses verwendet. Sowohl die Nutzung von LinkedIn als auch der Datenimport in Workday sind freiwillig. Für den Mitarbeiter entstehen durch das Unterlassen der genannten Funktionalität keine Nachteile; er nimmt wie jeder andere Mitarbeiter an den Talentförderungs- und Nachfolgeplanungsprozessen teil.

Jedwede Erhebung, Verarbeitung, Nutzung, Speicherung und Änderung von Daten darf nur im Rahmen der vorgenannten Funktionalitäten erfolgen."

Ziffer 6 der vorläufigen Gesamtbetriebsvereinbarung regelt abschließend die Daten, die im Rahmen der beschriebenen Zwecke erhoben und verarbeitet werden können; sie sind in Anlage 1 im Einzelnen aufgeführt. Was die Übermittlung angeht, so bestimmt Ziffer 6.4:

„Das Unternehmen wird sicherstellen, dass die Weitergabe von Daten an Dritte (zum Beispiel durch die Konzernmutter Sanofi SA) nur erfolgt, sofern dies rechtlich zulässig ist und das Unternehmen der Weitergabe ausdrücklich zugestimmt hat."

Ziffer 6.5 stellt fest, dass die Daten in Workday, die Sanofi betreffen, nach einem anerkannten Verfahren wirksam verschlüsselt sind. In Notfällen, in denen Workday auf die Daten zugreifen muss, bedarf es einer Genehmigung von SADG; auch muss ein bestimmter Account verwendet werden. Der Zugriff wird protokolliert und Sanofi kann auditieren, wenn ein solcher Zugriff erfolgt.

Die Zugriffsprofile sind in Anlage 3 dargestellt, wobei ein Rollenkonzept zugrunde gelegt wird. Dabei gibt es auch globale Zugriffsrollen, die für bestimmte Personen einen weltweiten Zugriff auf bestimmte Daten ermöglichen.

Ziffer 14 der vorläufigen Gesamtbetriebsvereinbarung gewährt dem Gesamtbetriebsrat Kontrollrechte, Ziffer 15 betrifft die Rechte der einzelnen Mitarbeiter, die von SADG Auskunft über alle zu ihrer Person gespeicherten Daten verlangen können. Ziffer 16 verbietet Leistungs- und Verhaltenskontrollen mit Hilfe von Workday. Rechtswidrig erworbene Informationen sind von der Verwertung in gerichtlichen Verfahren ausgeschlossen.

V. Der Entwurf einer Vereinbarung mit dem Unternehmenssprecherausschuss

Trotz verschiedener Entwürfe der Arbeitnehmerseite ist bisher keine Vereinbarung mit dem Unternehmenssprecherausschuss zustande gekommen. Die neueste Version eines

Entwurfs stammt vom 17. 3. 2015. In seiner Präambel benennt er eingangs die strategische Entscheidung des Konzerns, „zur Unterstützung der Personalarbeit weltweit“ das Personalinformationssystem Workday einzuführen und es zur „Personaldatenpflege“, zu „Leistung und Vergütung (Performance & Recognition)“ und zur „Talentförderung und Nachfolgeplanung (Talent Management & Succession Planning)“ einzusetzen. Geplant ist der Abschluss einer Vereinbarung, die unmittelbar und zwingend auf die Arbeitsverhältnisse der leitenden Angestellten einwirkt (§ 28 Abs. 2 Satz 1 SprAuG).

Der Entwurf enthält in Ziffer 4.2 Informationsrechte in Bezug auf die Auftragsdatenverarbeitung durch Workday und sieht in Ziffer 4.4 vor, dass Daten, die älter als drei Jahre sind, von diesem Zeitpunkt an gesperrt werden. Außerdem wird ausdrücklich unter Bezugnahme auf § 25 Abs. 1 Satz 2 SprAuG betont, dass die Rechte des einzelnen leitenden Angestellten unberührt bleiben.

Die Funktionalitäten des Personalinformationssystems Workday werden unter Ziffer 5 ähnlich beschrieben wie in der Gesamtbetriebsvereinbarung. Auch bei dem in Ziffer 6 behandelten Datenkatalog ergeben sich weitgehende Übereinstimmungen. Dasselbe gilt für die Zugriffsberechtigungen; eine Sonderregelung ist in Ziffer 8.7 für Fälle von missbräuchlichem Zugriff vorgesehen. Auch der Unternehmenssprecherausschuss verlangt Kontrollrechte (Ziffer 12) und die Anerkennung der Individualrechte der Leitenden Angestellten (Ziffer 13).

B. Rechtliche Fragestellungen

Die Workday überlassenen Daten wurden zuvor bereits innerhalb des Konzerns – etwa von Deutschland nach Frankreich – übermittelt. Davon geht auch das Datenschutzabkommen zwischen SADG und SAG aus, das sich nicht auf Fälle der Auftragsdatenverarbeitung beschränkt. Insbesondere im Bereich „Leistung und Vergütung“ sowie im Bereich „Talentförderung und Nachfolgeplanung“ gibt es ersichtlich einen Bedarf nach konzerneinheitlicher Planung und Entscheidung, was sich in der Existenz von einzelnen Personen mit globalen Zuständigkeiten niederschlägt. Dies ließe sich mit Hilfe einer bloßen Auftragsdatenverarbeitung nicht bewerkstelligen, da diese das Weisungsrecht zum Umgang mit den Daten bei der jeweiligen verantwortlichen Stelle, d. h. bei dem jeweiligen Konzernunternehmen belässt. Es liegt also notwendigerweise eine Übermittlung vor. Weiter sind die Workday zur Verfügung gestellten Daten zwar in Dublin und Amsterdam gespeichert, können jedoch auch von einzelnen Drittländern aus eingesehen und abgerufen werden. Dies stellt nach § 3 Abs. 4 Nr. 3b BDSG eine Übermittlung im Rechtssinne in diese Länder dar. Es wird zu prüfen sein, ob sowohl die Übermittlung in einen andern EU-Mitgliedstaat wie auch in einen Drittstaat im konkreten Fall mit datenschutzrechtlichen Vorschriften in Einklang steht.

Werden Daten von einem Konzernunternehmen an ein anderes übermittelt, bedarf es hierfür auch im Inland und zwischen zwei Unternehmen innerhalb der EU einer Rechtsgrundlage. Welche Vorschriften hierfür in Betracht kommen, soll unten unter C I erörtert werden.

Soweit Daten in ein Drittland übermittelt werden, das über kein angemessenes Datenschutzniveau verfügt, muss nach §§ 4b, 4c BDSG eine weitere Rechtsgrundlage hinzukommen. Diese kann in einer Genehmigung der Aufsichtsbehörde liegen, die aber nur dann erteilt wird, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes der Persönlichkeitsrechte der Betroffenen vorweist. Diese können im Abschluss eines EU-Mustervertrags, aber auch darin liegen, dass verbindliche Unternehmensregelungen über den Datenschutz auch für die Niederlassungen in Drittstaaten bestehen. Dies soll unten im Einzelnen unter C II ausgeführt werden.

Die Prüfung, ob eine zulässige Datenübermittlung vorliegt, ist daher bei multinationalen Konzernen mit Niederlassungen in Drittstaaten immer eine zweistufige: Zunächst müssen die allgemeinen Voraussetzungen für eine Übermittlung gegeben sein; anschließend muss dann als zweites geprüft werden, ob die spezifischen Bedingungen der Übermittlung in Drittstaaten erfüllt sind.

> Forst, in: Thüsing (Hrsg.), Beschäftigtendatenschutz und Compliance, 2. Aufl., München 2014, § 17 Rn. 15 (im Folgenden zitiert: Thüsing-Bearbeiter); Gola/Wronka, Handbuch Arbeitnehmerdatenschutz. Rechtsfragen und Handlungshilfen, 6. Aufl., Heidelberg-München u. a. 2013, Rn. 828: Schöttle, in: Weth/Herberger/Wächter (Hrsg.), Daten- und Persönlichkeitsschutz im Arbeitsverhältnis. Praxishandbuch zum Arbeitnehmerdatenschutz, München 2014, Teil C IV Rn. 5 (im Folgenden zitiert: Weth/Herberger/Wächter-Bearbeiter). Ebenso der Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer“ des Düsseldorfer Kreises, 2007, S. 15 (abrufbar unter https://www.datenschutz.hessen.de/bd001.htm - 7. 8. 2015)

Wie es sich damit im konkreten Fall verhält, wird im selben Abschnitt zu untersuchen sein.

Im Abschnitt C III sollen dann die Konsequenzen behandelt werden, die sich in der aktuellen Situation aus diesen datenschutzrechtlichen Rahmenbedingungen ergeben. Dies betrifft insbesondere die Frage nach dem Vorliegen einer ausreichenden Rechtsgrundlage für die konzerninterne Übermittlung. Weiter sind im Zusammenhang mit der Einführung von Workday eine Reihe von Einzelfragen aufgeworfen worden, die insbesondere die „freiwilligen“ Angaben betreffen, die der Einzelne in das System eingeben kann. Schließlich fragt sich, wie mit der Gefahr eines Zugriffs nach dem Patriot Act in den USA umzugehen ist.

C.) Rechtliche Stellungnahme

I. Konzerninterne Datenübermittlung im Inland

1. Das einzelne Konzernunternehmen als verantwortliche Stelle

Das deutsche Datenschutzrecht nimmt das Phänomen „Konzern“ nicht zur Kenntnis. Es unterscheidet sich insoweit vom Kartellrecht, vom Gesellschaftsrecht und vom Steuerrecht. Auch das Arbeitsrecht kennt spezielle Normen für den Konzern; in diesem Zusammenhang sei nur an die §§ 54 ff. BetrVG und die dort geregelte Existenz des Konzernbetriebsrats erinnert. Das BDSG stellt demgegenüber in § 2 Abs. 4 ausschließlich auf natürliche und juristische Personen ab, denen Gesellschaften und andere Personenvereinigungen des privaten Rechts gleichgestellt sind.
Das Fehlen eines „Konzernprivilegs“ ist in Rechtsprechung und Literatur allgemein anerkannt.

> S. statt aller Kramer in: Auernhammer (Begr.), Kommentar zum BDSG, 4. Aufl., Köln 2014, § 27 Rn. 10 (im Folgenden zitiert: Auernhammer-Bearbeiter); Plath, in: Plath (Hrsg.), BDSG-Kommentar, Köln 2013, § 28 Rn. 73 (im Folgenden zitiert: Plath-Bearbeiter); Schild, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, Kommentar, München 2013, § 3 Rn. 125 (im Folgenden zitiert: Wolff/Brink-Bearbeiter); Wolff/Brink-Schantz, § 4b Rn. 12; Simitis, in: Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014, § 2 Rn. 142 ff. (im Folgenden zitiert: Simitis-Bearbeiter); Wybitul/Schultze-Melling, Datenschutz im Unternehmen, 2. Aufl., Frankfurt/Main 2014, Grundzüge, Rn. 74

Verantwortliche Stelle im Rechtssinne ist daher auch eine Gesellschaft, die zu 100 % einer anderen Person oder Gesellschaft gehört und deren Handlungsspielräume sehr beschränkt sein können.

Die Anknüpfung an der rechtlich selbständigen Einheit hat zur Folge, dass die Datenübermittlung von einem Konzernunternehmen an ein anderes nach § 4 Abs. 1 BDSG einer besonderen Rechtsgrundlage bedarf – im Prinzip nicht anders, als würden die Daten

an ein beliebiges anderes Unternehmen übermittelt, zu dem keinerlei besondere gesellschaftsrechtliche Bindungen bestehen.

So ausdrücklich Bierekoven, in: Forgó/Helfrich/Schneider (Hrsg.), Betrieblicher Datenschutz. Rechtshandbuch, München 2014, Teil X Kap. 1 Rn. 31 (im Folgenden zitiert: Forgó/Helfrich/Schneider-Bearbeiter); Weth/Herberger/Wächter-Schoettle, Teil C IV Rn. 1

In der Unternehmenspraxis schafft dies nicht wenige Probleme, weil die wirtschaftliche Einheit „Konzern" nach einheitlichen Entscheidungen strebt, die sich häufig nur auf der Basis von Informationen treffen lassen, die von den einzelnen Konzernunternehmen geliefert werden. Der praktische Bedarf nach gesetzeskonformen Lösungen ist daher hoch.

So die Formulierung bei Auernhammer-Kramer § 27 Rn. 10

Bei Arbeitnehmerdaten kommt als Rechtsgrundlage für die konzerninterne Übermittlung § 32 Abs. 1 Satz 1 BDSG in Betracht, wonach Beschäftigtendaten an Dritte übermittelt werden dürfen, wenn dies u. a. zur Durchführung des Arbeitsverhältnisses erforderlich ist. Dazu unten 2.

Weiter ist zu prüfen, ob die Datenübermittlung auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden kann. Dies setzt voraus, dass es zur Wahrung „berechtigter Interessen" des Arbeitgebers erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Arbeitnehmers am Ausschluss der Übermittlung überwiegt. Dabei stellt sich die Vorfrage, ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG überhaupt neben § 32 Abs. 1 Satz 1 BDSG zur Anwendung kommen kann. Dazu unten 3.

Als Grundlage für eine Übermittlung kommt weiter eine Einwilligung des Arbeitnehmers nach § 4a BDSG in Betracht. Dazu unten 4.

Ein Datentransfer ist weiter auch dann gegeben, wenn innerhalb eines Konzerns eine Auftragsdatenverarbeitung im Sinne von § 11 BDSG vereinbart wird, doch ist ihr Anwendungsbereich relativ beschränkt. Näheres dazu unten 5.

Schließlich wird auch die Frage erörtert, ob eine Konzernbetriebsvereinbarung nicht eine Rechtsgrundlage für eine konzerninterne Datenübermittlung sein kann, sofern man sie als „andere Rechtsvorschrift“ im Sinne des § 4 Abs. 1 BDSG ansehen kann, die für diesen Fall aber möglicherweise bestimmten inhaltlichen Vorgaben Rechnung tragen muss. Dazu unten 6.

Sonderregeln bestehen in Bezug auf sensitive Daten nach § 3 Abs. 9 BDSG (unten 7).

2. Konzerninterne Datenübermittlung auf der Grundlage des § 32 Abs. 1 Satz 1 BDSG

Soweit eine Datenübermittlung für die Durchführung eines Arbeitverhältnisses erforderlich ist, darf sie stattfinden. Dies bedeutet, dass dann, wenn sich das Arbeitsverhältnis nicht nur auf den Vertragsarbeitgeber bezieht, sondern „konzerndimensionalen“ Charakter besitzt, auch die Datenübermittlung in diesem erweiterten Bereich stattfinden kann. Dies ist insbesondere dann der Fall, wenn sich die Tätigkeit des Arbeitnehmers nach dem Arbeitvertrag auch auf andere Konzernunternehmen erstreckt.

Ebenso die praktisch allgemein geteilte Auffassung. S. etwa Auernhammer-Forst, § 32 Rn. 43 und Auernhammer-Thomale § 4c Rn. 5; Däubler, Gläserne Belegschaften? Das Handbuch zum Arbeitnehmerdatenschutz, 6. Aufl., Frankfurt/Main 2015, Rn. 454; Gola RDV 2002, 114; Gola/Wronka Rn. 810; Forgó/Helfrich/Schneider- Moos/Zeiter, Teil V Kap. 1 Rn. 18, 21; Plath-Stamer/Kuhnke, § 32 Rn. 143; Ruppmann, Der konzerninterne Austausch personenbezogener Daten. Risiken und Chancen für den Datenschutz, Baden-Baden 2000, S. 60; Simitis-Seifert § 32 Rn. 118; Zöll, in: Taeger/Gabel (Hrsg.), BDSG und Datenschutzvorschriften des TKG und TMG, 2. Aufl., Frankfurt/Main 2013, § 32 Rn. 39 (im Folgenden zitiert: Taeger/Gabel-Bearbeiter).

Wer in seinem Arbeitvertrag beispielsweise eine wirksame Klausel hat, wonach er auch in anderen Konzernunternehmen eingesetzt werden kann (was insbesondere bei Führungskräften vorkommen wird), schafft damit zugleich eine Rechtsgrundlage dafür,

dass seine Daten beispielsweise an die Konzernspitze übermittelt werden, damit diese ggf. bei Bedarf von ihrem Versetzungsrecht Gebrauch machen kann. Ein tatsächlicher Wechsel des Arbeitsorts muss noch nicht stattgefunden haben.

So auch Taeger/Gabel-Zöll § 32 Rn. 39; zur Zulässigkeit der Konzernversetzungsklausel s. Däubler, in: Däubler/Bonin/Deinert, AGB-Kontrolle im Arbeitsrecht, 4. Aufl., München 2014, Anhang Rn. 324

Von einigen Autoren wird der „Konzernbezug" recht weit interpretiert, was die Möglichkeiten zur Datenübermittlung vergrößert. So soll es genügen, dass bei der Einstellung der mögliche Einsatz in anderen Konzernunternehmen „klar ersichtlich" ist,

so Weth/Herberger/Wächter-Schöttle C IV Rn. 8

oder wenn in einem Projektteam mit Kollegen aus unterschiedlichen Konzernunternehmen zusammengearbeitet wird.

Gola/Wronka, Rn. 812

Der Arbeitsbericht der Ad-hoc-Arbeitsgruppe „konzerninterner Datentransfer" will es insbesondere bei Führungskräften sogar genügen lassen, dass ihnen bei der Einstellung die Notwendigkeit der Mobilität innerhalb des Konzerns bewusst ist; dasselbe soll ganz generell für Nachwuchskräfte gelten, die sich auf Führungsaufgaben vorbereiten.

Regierungspräsidium Darmstadt/Hillenbrand-Beck, Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer", S. 6 (abrufbar unter http://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/5_Beschaeftigtendatenschutz_Konzern/arbeitspapier_ad_hoc_idv. pdf)

Nach einer weiteren Auffassung soll es genügen, dass die konzernweite Personalverwaltung schon bei der Einstellung bekannt war.

Plath-Stamer/Kuhnke § 32 Rn. 145

Ob dem generell zugestimmt werden kann, erscheint zweifelhaft: Am Ende könnte eine solche „konzernfreundliche“ Auslegung des Arbeitsvertrages dazu führen, dass von der gesetzlichen Entscheidung zugunsten der „Informationseinheit Unternehmen“ kaum mehr etwas übrig bliebe, weil man die subjektive Kenntnis von Konzernzusammenhängen unschwer unterstellen kann. Nach hier vertretener Auffassung ist der Arbeitsvertrag nur dann eine taugliche Grundlage für eine konzerninterne Datenübermittlung, wenn er diese auch effektiv notwendig macht. Dies ist bei einem vertraglich ermöglichten Einsatz in einem andern Konzernunternehmen der Fall, nicht aber dann, wenn die Konzernstrukturen oder eine konzerneinheitliche Personalverwaltung bei der Einstellung bekannt sind.

Letztlich kann im vorliegenden Zusammenhang die Frage aber dahinstehen, da es immer eine Reihe von Beschäftigten geben wird, deren Arbeitsverhältnis auch bei großzügiger Betrachtung keinen Konzernbezug aufweist. Weiter ist an Personen zu denken, die bei den Farbwerken Hoechst bereits zu einem Zeitpunkt beschäftigt waren, als diese noch ein selbständiges Unternehmen war, so dass die Arbeitsverträge keinen Bezug auf die heutige Konzernstruktur aufweisen konnten. Auch eine konkludente nachträgliche Änderung wird sich schwerlich belegen lassen. Zumindest insoweit muss nach einer anderen Rechtsgrundlage gesucht werden.

3. Konzerninterne Datenübermittlung auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 2 BDSG

a) Das Verhältnis von § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu § 32 Abs. 1 Satz 1 BDSG

Ob § 28 Abs. 1 Satz 1 Nr. 2 BDSG bei Beschäftigtendaten überhaupt Anwendung finden kann, ist in der Literatur durchaus umstritten. Die zahlenmäßig leicht überwiegende Auffassung geht davon aus, dass § 32 Abs. 1 Satz 1 eine abschließende Sonderregelung für Beschäftigtendaten darstellt.

Für Vorrang des § 32 Simitis-Simitis § 2 Rn. 156; Franzen, in: Müller-Glöge/Preis/Schmidt (Hrsg.), Erfurter Kommentar zum Arbeitsrecht, 15. Aufl., München 2015, § 32 Rn. 3 (im Folgenden: ErfK-Bearbeiter); Däubler, Gläserne

Belegschaften? Rn. 185 und in: Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz. Kommentar, 4. Aufl., Frankfurt/Main 2014, § 32 Rn. 8 ff.; Weth/Herberger/Wächter-Schöttle Teil C II Rn. 35; Weichert, AuR 2010, 101; Simitis-Seifert § 32 Rn. 17; Wolff/Brink-Wolff, § 28 Rn. 3; im Ergebnis auch Gola/Schomerus, BDSG, 12. Aufl., München 2015, § 32 Rn. 50 und Plath-Plath, § 28 Rn. 73.

Für Anwendung des § 28 Abs. 1 Satz 1 Nr. 2 neben § 32 BDSG Forst NZA 2010, 427, 431; Taeger/Gabel-Zöll, § 32 Rn. 40; Rolf/Rötting RDV 2009, 263 ff.; Lembke, in Henssler/Willemsen/Kalb, Arbeitsrecht. Kommentar, 6. Aufl., Köln 2014, § 32 Rn. 4 (im Folgenden zitiert: HWK-Bearbeiter); Forgó/Helfrich/Schneider-Moos/Zeiter, Teil V Kap. 1 Rn. 24; Wolff/Brink-Riesenhuber § 32 Rn. 30; Wybitul/Schultze-Melling, Grundzüge, Rn. 74.

Eher unentschieden Thüsing-Thüsing § 3 Rn. 30; Auernhammer-Forst § 32 Rn. 14 – 16

Die herrschende Meinung lässt sich insbesondere auf das Argument stützen, dass die Anwendung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu einem Konzernprivileg „durch die Hintertüre“ führen würde,

So Gola/Wronka, Rn. 815

dies jedenfalls dann, wenn man bereits das „Zusammenführungsinteresse“ der Konzernunternehmen als „berechtigtes Interesse“ im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG qualifizieren würde.

Plath-Plath § 28 Rn. 73: Berechtigtes Interesse darf nicht allein aus der Konzernverbundenheit abgeleitet werden.

Damit würde die Grundentscheidung des Gesetzgebers gegen den Konzern als Informationseinheit weitgehend rückgängig gemacht. Auch würde ein ungehinderter Informationsfluss im Konzern schutzwürdige Interessen der Beschäftigten verletzen, weil

die Datentransparenz verloren ginge: Oft ist dem Einzelnen nicht einmal bekannt, welche Unternehmen im Einzelnen zum Konzern gehören.

Simitis-Simitis § 2 Rn. 156, 157

Dazu kommen weitere Gesichtspunkte. In der Amtlichen Begründung zum BDSG-Änderungsgesetz von 2009 heißt es zunächst, § 32 Abs. 1 gehe dem § 28 Abs. 1 Satz 1 Nr. 1 BDSG vor, doch schon wenige Sätze weiter wird ausgeführt (BT-Drucksache 16/13657 S. 35):

„Werden personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt, findet § 28 Abs. 1 keine Anwendung mehr. Für andere Zwecke können auch im Verhältnis von Arbeitgeber und Beschäftigten die Vorschriften des Bundesdatenschutzgesetzes und anderer Gesetze, die eine Datenerhebung, -verarbeitung und -nutzung erlauben oder anordnen, weiterhin Anwendung finden. Dazu gehören die Regelungen über die Datenerhebung, -verarbeitung und -nutzung zur Wahrung berechtigter Interessen des Arbeitgebers (§ 28 Absatz 1 Satz 1 Nummer 2) und über die Datenübermittlung und -nutzung zur Wahrung berechtigter Interessen eines Dritten (§ 28 Absatz 3 Satz 1 Nummer 1).“

Daraus muss man den Schluss ziehen, dass der durch den Arbeitvertrag gezogene Rahmen Verbindlichkeit beansprucht, also nicht durch Rückgriff auf die Nummer 2 von § 28 Abs. 1 Satz 1 erweitert werden kann.

Vgl. auch Reichold, in: Richardi u. a. (Hrsg.), Münchener Handbuch zum Arbeitsrecht, 3. Aufl., München 2009, § 88 Rn 29 (im Folgenden zitiert: MünchArbR-Bearbeiter), der für das frühere Recht zutreffend die Auffassung vertritt, soweit ein Vertrag vorliege, bestimme dieser die Verarbeitungsgrenze, auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 könnten dann keine weiter gehenden Informationen gewonnen werden.

Verfolgt der Arbeitgeber mit der Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten dagegen andere Zwecke, will er beispielsweise Verhandlungen mit

einem potentiellen Betriebserwerber durch Rückgriff auf Mitarbeiterdaten fördern, so richtet sich die Zulässigkeit seines Vorgehens nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Für die hier vertretene Auslegung spricht auch die gesetzliche Systematik. Das in § 28 Abs. 1 Satz 1 Nr. 2 BDSG angesprochene „berechtigte Interesse“ der verantwortlichen Stelle, das gegen die schutzwürdigen Interessen des Betroffenen abzuwägen ist, findet sich im Erforderlichkeitsgrundsatz von § 32 Abs. 1 Satz 1 BDSG wieder.

> Ebenso Gola/Schomerus § 32 Rn. 50

Dem Arbeitgeber die Möglichkeit zu eröffnen, für Zwecke des Arbeitsverhältnisses Daten zu verarbeiten, die außerhalb des Erforderlichen nach § 32 Abs. 1 Satz 1 BDSG liegen, wäre ersichtlich eine vom Gesetzgeber nicht gewollte innere Inkonsequenz. Die schlichte Erweiterung um nicht erforderliche Daten wird (vermutlich ungewollt) in einer „Praxishilfe“ des GDD-Arbeitskreises Datenschutzpraxis deutlich, wo es heißt:

> „§ 28 Abs. 1 Satz 1 Nr. 2 BDSG kann im Ausnahmefall eine Datenübermittlung rechtfertigen, wenn es um Vorgänge mit Bezug zum Arbeitsverhältnis geht, die jedoch bei enger Interpretation nicht mehr der Zweckbestimmung des Vertragsverhältnisses zuzuordnen sind.“ (GDD-Arbeitskreis „Datenschutz-Praxis“ Praxishilfe V, Mitarbeiterdaten im Unternehmensverbund, 2. Aufl. 2014, S. 7 – abrufbar unter https://www.gdd.de/downloads/materialien/europ_datenschutztag/eu-ds-tag_2014/GDDPraxishilfe_V_2.Aufl.pdf, zuletzt abgerufen am 7. 8. 2015)

b.) Situation bei Anwendbarkeit des § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Geht man mit der Gegenmeinung davon aus, dass der Arbeitgeber nicht auf die „erforderliche“ Datenübermittlung nach § 32 Abs. 1 Satz 1 beschränkt ist, sondern auch weitergehende Verarbeitungsrechte hat, so ist zu prüfen, ob er sich auf ein berechtigtes Interesse stützen kann und keine schutzwürdigen Belange des Arbeitnehmers entgegen stehen. In der Literatur wird ohne Benennung konkreter Rechtsgrundlagen die Auffassung vertreten, für die Arbeitnehmerbelange müsse Vorsorge getroffen werden. So dürfe die Datenübermittlung nicht dazu führen, dass die neue verantwortliche Stelle zusätzliche

Befugnisse erhalte, die der Arbeitgeber nicht habe. Außerdem müsse dafür gesorgt werden, dass die Individualrechte nach den §§ 33 bis 35 BDSG (Auskunft, Berichtigung, Löschung, Sperrung) und die Haftung nach §§ 7, 8 BDSG nicht nur – wie es dem Gesetz entspricht – dem Datenempfänger gegenüber geltend gemacht werden können; vielmehr sei auch der Arbeitgeber verpflichtet, weiterhin für ihre Realisierung Sorge zu tragen.

> Taeger/Gabel-Zöll § 32 Rn. 40; ähnlich Forgó/Helfrich/Schneider-Moos/Zeiter, Teil V Kap. 1 Rn. 26. S. auch Arbeitsbericht „Konzerninterner Datentransfer", S. 8: Arbeitgeber muss umfassender Ansprechpartner bleiben.

Auf diese Weise könne auch dem Transparenzprinzip Rechnung getragen werden, dessen Wahrung ja hinter der Nichtberücksichtigung des Konzerntatbestandes steht.

Im Ergebnis läuft diese Auffassung darauf hinaus, dass sich für den Einzelnen faktisch nichts zu ändern scheint: Der Arbeitgeber wird ihm alle Informationen geben, die er notfalls durch Rückfrage beim Datenempfänger in Erfahrung bringen muss. In Wirklichkeit erweitern sich die Befugnisse der Arbeitgeberseite, weil personenbezogene Daten aus (vielen) anderen Konzernunternehmen als Vergleichsmaterial herangezogen werden können. Es macht für den Betroffenen ersichtlich einen erheblichen Unterschied, ob er beispielsweise im Rahmen der Nachwuchsförderung nur mit 40 anderen Beschäftigten seines Arbeitgebers verglichen werden kann oder ob er mit 500 anderen Arbeitnehmern um Fortbildungskurse und Aufstiegschancen konkurriert. Auch ist es nicht unwichtig, ob man bei fehlender Zielerreichung zu einer Minderheit von 20 % im Unternehmen gehört oder ob es konzernweit nur 3 % solcher Fälle gibt. Insofern ist die Anforderung „keine zusätzlichen Befugnisse für den Datenempfänger" in der Praxis nicht einzuhalten. Sie kann nur dann funktionieren, wenn vom Mittel der Auftragsdatenverarbeitung Gebrauch gemacht wird, um die es aber hier nicht geht.

Zu denken ist weiter daran, ein „berechtigtes Interesse" des Arbeitgebers nicht schon dann zu bejahen, wenn es ganz allgemein um das wirtschaftliche Wohlergehen des Konzerns, also beispielsweise um eine kleine Verbesserung des Deckungsbeitrags einer Abteilung geht. Vielmehr müsste ein gewichtigeres Interesse auf dem Spiel stehen, das etwa darin liegen könnte, strafbare Handlungen aufzuklären oder die Experten verschiedener

Unternehmen zu bestimmten (Forschungs-)Fragen zusammenzuführen. Bisher sind solche Überlegungen aber in der Literatur nicht angestellt worden.

Als Zwischenergebnis ist festzuhalten, dass § 28 Abs. 1 Satz 1 Nr. 2 BDSG hinter § 32 Abs. 1 Satz 1 BDSG zurücktritt und deshalb keine Rechtsgrundlage für eine konzerninterne Datenübermittlung darstellt. Sieht man dies mit der Mindermeinung anders, muss dafür gesorgt werden, dass die Arbeitnehmer möglichst geringe Eingriffe in ihre Persönlichkeitssphäre hinnehmen müssen. Erforderlich ist insbesondere, dass sie alle Individualrechte auch gegenüber ihrem Arbeitgeber geltend machen können.

4. Einwilligung des Arbeitnehmers in die konzerninterne Datenübermittlung

Nach § 4 Abs. 1 BDSG ist eine Datenübermittlung auch dann rechtmäßig, wenn der Betroffene zuvor eingewilligt hat. Die Einwilligung hat nach § 4a BDSG allerdings nur wirksam, wenn sie eine ganze Reihe von Voraussetzungen erfüllt.

> Dazu im Einzelnen Däubler, Gläserne Belegschaften? Rn. 135 ff.; Gola/Schomerus § 4a Rn. 1 ff.; Taeger/Gabel-Taeger § 4a Rn. 1 ff.

Die im vorliegenden Zusammenhang bedeutungsvollsten seien hier aufgeführt.

- Der Beschäftigte muss sich bewusst sein, überhaupt eine Einwilligung abzugeben. Daran fehlt es, wenn er die Bedeutung seiner Entscheidung nicht übersieht (ihm fehlt z. B. die nötige Einsichtsfähigkeit) und erst recht dann, wenn er bei der Beantwortung bestimmter Fragen der Auffassung ist, eine vertragliche Verpflichtung zu erfüllen und nicht etwa eine freiwillige Erklärung abzugeben.

- Die Einwilligung muss bestimmten formalen Anforderungen entsprechen. Sie muss vor dem fraglichen Vorgang abgegeben werden und im Regelfall schriftlich erfolgen. Wegen besonderer Umstände kann eine andere Form angemessen sein, was insbesondere dann der Fall ist, wenn eine langjährige Geschäftsbeziehung besteht und deshalb nicht bei jeder Datenübermittlung eine neue schriftliche Erklärung abgegeben werden sollte.

> Gola/Schomerus, § 4a Rn. 29a

Dies ist aber nur dann der Fall, wenn es um Routinemaßnahmen geht; würden neue Daten übermittelt, die bisher keine Rolle spielten, wäre die Schriftform selbstredend einzuhalten. „Schriftform“ bedeutet nach § 126 BGB eigenhändige Unterschrift; wenn die technischen Voraussetzungen gegeben sind, kann auch eine elektronische Signatur genügen (§ 126a BGB).

- Nach § 4a Abs. 1 Satz 2 BDSG muss der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen werden. Je nach der beabsichtigten Datenverarbeitung läuft dies auf unterschiedlich weit reichende Informationspflichten hinaus, die von einem eher pauschalen Hinweis („Ihre Stammdaten werden die die Konzernmutter übermittelt“) bis zu umfassender Aufklärung („Die Einfügung Ihrer Daten in das Talent Management System kann dazu führen, dass Sie bei Beförderungen berücksichtigt, aber auch nicht berücksichtigt werden“) reichen können.

Einzelheiten bei Hartmann DuD 2008, 455, 459

Auch auf die Folgen einer Verweigerung muss der Betroffene hingewiesen werden. Ein Hinweis darauf kann nur entfallen, wenn diese auf der Hand liegen.

AG Elmshorn RDV 2005, 174 = CR 2005, 641

Dies wäre etwa dann der Fall, wenn im Betrieb allgemein bekannt ist, dass über den Aufstieg in bestimmte Positionen konzernweit entschieden wird und dass die Eintragungen in eine bestimmte unternehmensübergreifende Datei dabei eine mehr oder weniger große Rolle spielen.

- Die Einwilligung muss eindeutig sein. Ist sie in einem Vertragstext, insbesondere in Allgemeinen Geschäftsbedingungen erhalten, so ist sie nach § 4a Abs. 1 Satz 4 BDSG (in der Regel drucktechnisch) besonders hervorzuheben.

- Die Einwilligung darf nach allgemeiner Auffassung keinen pauschalen Charakter haben. Sie muss erkennen lassen, in die Speicherung und Verarbeitung welcher Daten eingewilligt wird; der Betroffene muss insoweit den Überblick behalten können.

Dieses Bestimmtheitserfordernis wäre nicht gewahrt, wenn der Betroffene etwa erklären würde, er sei mit dem Transfer aller seiner Daten an die Konzernspitze einverstanden.

Zum Bestimmtheitserfordernis näher Klug RDV 2001, 272; MünchArbR-Reichold § 88 Rn. 23; Simitis-Simitis § 4a Rn. 77 ff.; Wohlgemuth BB 1996, 693; Däubler/Klebe/Wedde/Weichert-Däubler § 4a Rn. 18 f.

- Nach § 4a Abs. 1 Satz 1 BDSG muss die Einwilligung auf der „freien Entscheidung" des Betroffenen beruhen. Ob und wann diese Voraussetzung bei Arbeitnehmern und sonstigen Beschäftigten gegeben ist, erscheint nicht voll geklärt. Auf der einen Seite wird die Freiwilligkeit nur verneint, wenn der Betroffene getäuscht oder bedroht wurde, wenn ihm insbesondere bestimmte Nachteile in Aussicht gestellt werden. Auf der anderen Seite vertrat der Hamburgische Datenschutzbeauftragte die Auffassung, dem Arbeitnehmer fehle generell die Unabhängigkeit, um eine wirksame Einwilligung abgeben zu können.

Hamburgischer Datenschutzbeauftragter, 18. Tätigkeitsbericht, S. 197

Dies erscheint als zu schematische Auffassung. Ohne hier die Diskussion in allen Einzelheiten wiedergeben zu können, lässt sich im Anschluss an anderwärts gemachte Ausführungen

Däubler, Gläserne Belegschaften? Rn. 160

am ehesten eine differenzierende Auffassung vertreten. Danach ist die Freiwilligkeit nur gewahrt, wenn

die Willensbildung des Betroffenen nicht in unangemessener Weise beeinflusst wurde (z. B. durch „Überrumpelung" oder einseitige Beratung) und wenn

keine vermeidbaren Nachteile und

keine übermäßigen Vorteile

in Aussicht gestellt wurden.

Ebenso Tinnefeld DuD 2002, 233

Dem „In-Aussicht-Stellen“ entspricht der Fall, dass der Betroffene den Umständen nach davon ausgehen konnte, bei einem „Nein“ würden ihm ernsthafte Nachteile drohen. Unproblematisch ist in aller Regel der Fall, dass mit der Preisgabe der Daten eine Maßnahme ermöglicht werden soll, die dem Arbeitnehmer ausschließlich oder vorwiegend Vorteile bringt.

- Einwilligungen werden häufig in standardisierter Form erteilt, sei es, dass sie Bestandteil einheitlicher Arbeitsverträge, sei es, dass ihr Wortlaut aus einem bestimmten Anlass heraus vom Arbeitgeber vorformuliert wurde. In beiden Fällen findet die AGB-Kontrolle nach §§ 305 bis 310 BGB Anwendung.

Dazu auch BGHZ 98, 28: Einseitige Rechtsgeschäfte des Verbrauchers, die vom Unternehmer vorformuliert sind, werden gleichfalls als AGB behandelt. Ebenso BGHZ 141, 124. Wie hier Thüsing-Thüsing/Traut § 5 Rn. 25 ff.; Plath-Plath § 4a Rn. 39. Beispielsfälle bei Heidemann/Peuser DuD 2002, 393

Eine unangemessene Benachteiligung im Sinne des § 307 Abs. 1 BGB läge beispielsweise vor, wenn die durch Einwilligung legitimierte Datenverarbeitung ersichtlich keinen berechtigten Interessen des Arbeitgebers entspricht, wenn dieser beispielsweise die Beschäftigtendaten lediglich an einen Adresshändler verkaufen möchte.

- In einem Konzern kann zweifelhaft sein, ob sich eine einmal gegebene Einwilligung auch auf neu hinzukommende Unternehmen erstreckt. Dies wird man bejahen können, sofern sich dadurch nicht der Zweck der möglichen Verarbeitungen insgesamt ändert.

Gola/Schomerus, § 4a Rn. 3; Plath-Plath § 4a Rn. 79;
Däubler/Klebe/Wedde/Weichert-Däubler, § 4a Rn. 45.

- Nach allgemeiner Auffassung ist die einmal erteilte Einwilligung widerruflich.

Bergmann/Möhrle/Herb, Datenschutzrecht. Handkommentar, Loseblatt, § 4a Rn. 24; Buchner, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006, S. 232; ErfK-Franzen, § 4a BDSG Rn. 4; Klug, RDV 2001, 272; HWK-Lembke, Vorb. BDSG Rn. 58; Schaar, MMR 2001, 647; MünchArbR-Reichold, § 88 Rn. 23; Simitis-Simitis, § 4a Rn. 94; Taeger/Gabel-Taeger, § 4a Rn. 81; Thüsing-Thüsing/Traut, § 5 Rn. 32; Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht, 5. Aufl., München 2012, S. 360

Dies hängt mit ihrem Persönlichkeitsbezug zusammen; der Einzelne soll die Möglichkeit haben, eine vorschnell getroffene Entscheidung wieder zu korrigieren. Der Widerruf ist formlos möglich. Ist die Einwilligung zum Gegenstand eines Vertrages gemacht worden, kann ihr Widerruf eine Verletzung der übernommenen Pflichten darstellen. Angesichts der persönlichkeitsrechtlichen Natur der Einwilligung ist aber nicht zu vermuten, dass die Beteiligten eine solche Bindung gewollt haben. Diese muss sich eindeutig aus dem Wortlaut oder den Umständen ergeben.

Die zahleichen Voraussetzungen, die eine wirksame Einwilligung zu erfüllen hat, haben zu der Empfehlung an Personalabteilungen geführt, von diesem Mittel möglichst keinen Gebrauch zu machen. Dabei wird insbesondere auf das Erfordernis der Freiwilligkeit, den Bestimmtheitsgrundsatz und das Widerrufsrecht abgestellt – die Ungewissheit, ob eine Erklärung wirklich freiwillig im Rechtssinne ist, ob sie präzise genug ist und ob schließlich ein Widerruf unterbleibt, lässt dieses Gestaltungsmittel als wenig praktikabel erscheinen.

So ausdrücklich Forgó/Helfrich/Schneider-Moos/Zeiter, Teil V Kap. 1 Rn. 33. Der Arbeitsbericht „Konzerninterner Darentransfer“ vertritt gleichfalls die Auffassung, in der Regel scheide die Einwilligung als Gestaltungsmittel aus (S. 7). Die GDD-Praxishilfe verweist mit gleicher Tendenz auf das Widerrufsrecht (S. 10).

Dies schließt nicht aus, dass in einem Konzern gleichwohl dort darauf zurückgegriffen wird, wo sich für Arbeitnehmer wie ggf. bei einem Stock-option-Plan ausschließlich Vorteile ergeben.

5. Auftragsdatenverarbeitung

Die Auftragsdatenverarbeitung belässt die Verantwortung für die Daten beim Auftraggeber und schaltet den Auftragnehmer nur zu dem Zweck ein, dass er mit seinen technischen Mitteln nach Weisung des Auftraggebers bestimmte Formen der Datenerhebung oder Datenverarbeitung durchführt. Die Voraussetzungen, die an ein Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer zu stellen sind, ergeben sich aus § 11 BDSG.

Auftragsdatenverarbeitung ist nach allgemeiner Auffassung auch innerhalb eines Konzerns möglich. Als Beispiel wird etwa die Gehaltsabrechnung genannt, mit deren technischer Durchführung ein bestimmtes Konzernunternehmen betraut wird.

Taeger/Gabel-Zöll § 32 Rn. 40; Taeger/Gabel-Gabel § 11 Rn. 23

Auch die Muttergesellschaft der konzernverbundenen Unternehmen kann Auftragnehmer sein, doch dürfen keine Anhaltspunkte dafür bestehen, dass diese Weisungen in Bezug auf die fraglichen Daten erteilt und auf diese Weise die Entscheidungsbefugnis der Tochtergesellschaft partiell oder ganz wieder aufhebt.

Taeger/Gabel-Gabel § 11 Rn. 22; Forgó/Helfrich/Schneider-Moos/Zeiter Teil V Kap. 1 Rn. 14

Werden die inhaltlichen Entscheidungsbefugnisse über den Umgang mit den Daten auf den Auftragnehmer übertragen, so liegt keine Auftragsdatenverarbeitung mehr vor. Vielmehr handelt es sich dann um eine Funktionsübertragung; eine bestimmte Aufgabe wird nicht mehr vom Arbeitgeber sondern von einer anderen Einheit erledigt. Insoweit liegt dann eine Datenübermittlung vor; § 11 BDSG findet keine Anwendung mehr. Die Abgrenzung ist nicht immer ganz unproblematisch. So ist etwa der Rahmen der Auftragsdatenverarbeitung noch nicht gesprengt, wenn die Personalverwaltung anhand feststehender Kriterien auf ein anderes Konzernunternehmen übertragen wird, doch ist die Grenze zur Funktionsübertragung eindeutig überschritten, wenn der Datenempfänger zur eigenständigen Erledigung der Aufgabe ermächtigt wird.

Taeger/Gabel-Gabel § 11 Rn. 23; Thüsing-Thüsing/Granetzny § 16 Rn. 21 ff.; Forgó/Helfrich/Schneider-Moos/Zeiter Teil V Kap. 1 Rn. 13 ff. S. auch Arbeitsbericht „Konzerninterner Datentransfer“ S. 3 ff.

Soweit die Arbeitgeberseite die Absicht hat, nicht nur einzelne technische Vorgänge, sondern auch Entscheidungskompetenzen zu zentralisieren, ist die Auftragsdatenverarbeitung kein taugliches Mittel.

6. Konzernbetriebsvereinbarung und Konzernsprechervereinbarung als Rechtsgrundlage

Als mögliche Rechtsgrundlage für die konzerninterne Datenübermittlung kommt schließlich eine vom Konzernbetriebsrat abgeschlossene Konzernbetriebsvereinbarung in Betracht. Zwar existiert bei SADG nur ein Unternehmen, dessen Belegschaft durch einen Gesamtbetriebsrat vertreten wird, doch ist es gleichwohl sinnvoll, diesen Punkt zu vertiefen: Soweit die Konzernbetriebsvereinbarung innerstaatlich eine ausreichende Rechtsgrundlage für die Übermittlung an ein anderes Konzernunternehmen darstellt, ist sie dies im Verhältnis zu ausländischen Konzernunternehmen auch eine Gesamtbetriebsvereinbarung, sofern die Voraussetzungen des Datentransfers ins Ausland erfüllt sind (zur Zweistufigkeit der Prüfung s. oben B). Die Konzernsprechervereinbarung ist wie eine Konzernbetriebsvereinbarung zu behandeln, soweit sie sich nach § 28 Abs. 2 Satz 1 SprAG unmittelbare und zwingende Wirkung beimisst.

Als erstes stellt sich die Frage, ob eine Betriebsvereinbarung eine „andere Rechtsvorschrift“ im Sinne des § 4 Abs. 1 BDG ist, die eine Datenverarbeitung erlauben kann. Die Rechtsprechung des BAG hat mit Rücksicht auf die unmittelbare und zwingende Wirkung der Normen von Betriebsvereinbarungen anerkannt, dass es sich insoweit um Rechtsvorschriften nach § 4 Abs. 1 BDSG handelt.

BAG NZA 1986, 643; BAG NZA 1996, 218, 221 linke Spalte unten; BAG NZA 1996, 945, 947 rechte Spalte

Auch die Literatur hat sich dem im Wesentlichen angeschlossen.

Auernhammer-Forst, § 32 Rn. 106; Däubler/Klebe/Wedde/Weichert-Weichert, § 4 Rn. 2; Gola/Wronka, Rn. 823; Forgó/Helfrich/Schneider-Hanloser, Teil IV Kap. 1 Rn. 15; Forgó/Helfrich/Schneider-Moos/Zeiter, Teil V Kap. 1 Rn. 30; Gola/Schomerus, § 4 Rn. 7, 10; Simitis-Scholz/Sokol, § 4 Rn. 11; Plath-Stamer/Kuhnke, § 32 Rn. 145; Thüsing-Thüsing/Forst, § 17 Rn. 3; Weth/Herberger/Wächter-Schöttle, Teil C III Rn. 55. Ebenso der Arbeitsbericht „Konzerninterner Datentransfer", S. 11 und die GDD-Praxishilfe, S. 4

Davon ist die weitergehende Frage zu unterscheiden, ob eine Betriebsvereinbarung Datenverarbeitungen wie z. B. konzerninterne Übermittlungen zulassen kann, die nach dem BDSG nicht zulässig wären. Die Meinungen in der Literatur sind geteilt. Die eine Auffassung verneint eine solche Möglichkeit und beschränkt die Betriebsparteien darauf, die recht allgemeinen Begriffe des BDSG wie „berechtigtes Interesse" und „schutzwürdige Belange" im Einzelnen zu konkretisieren und an die betrieblichen Verhältnisse anzupassen.

So Simitis-Scholz/Sokol § 4 Rn. 17; Hummel/Hilbrans AuR 2005, 207, 208; Fitting, Betriebsverfassungsgesetz. Handkommentar, 27. Aufl., München 2014, § 83 Rn. 30; Hilber RDV 2005, 143, 148; Däubler/Klebe/Wedde/Weichert-Weichert § 4 Rn 2; Rose DuD 2011, 136; Brandt DuD 2010, 213; Kort EDV 2012, 15; wohl auch Gola/Schomerus § 4 Rn. 10

Dem steht eine zweite Meinung entgegen, die eine Betriebsvereinbarung als sonstige Rechtsvorschrift betrachtet, die unabhängig von den Regelungen des BDSG eine Datenverarbeitung (einschließlich Datenübermittlung) zulassen kann.

So Auernhammer-Forst, § 32 Rn. 109; Wolff/Brink-Bäcker § 4 Rn 14; Weth/Herberger/Wächter-Schöttle Teil C III Rn. 55; Taeger/Gabel-Taeger § 4 Rn. 44

Sie kann sich dabei auf die Rechtsprechung des BAG stützen, das in einer älteren Entscheidung zur Telefondatenerfassung eine Abweichung „nach unten" zugelassen hatte, um so einen einheitlichen Verarbeitungsrahmen im Verhältnis zwischen Arbeitgeber und Belegschaft zu schaffen.

BAG AP Nr. 15 zu § 87 BetrVG 1972 Überwachung

In einer ungefähr zehn Jahre später ergangenen Entscheidung ging es um die Frage, ob der Konzernbetriebsrat befugt sei, eine Konzernbetriebsvereinbarung über den konzerninternen Datentransfer zu schließen. Diese Frage wurde bejaht und zugleich darauf verwiesen, die Konzernbetriebsvereinbarung sei eine „sonstige Rechtsvorschrift" nach § 4 Abs. 1 BDSG. Hätte das Gericht inhaltliche Bedenken gegen die getroffene Abmachung gehabt, hätte es diese zum Ausdruck bringen müssen; insbesondere wäre eine Subsumtion unter § 4 Abs. 1 BDSG bei einer unwirksamen Betriebsvereinbarung nicht möglich gewesen.

BAG 20. 12. 1995 – 7 ABR 8/95 – NZA 1996, 945

Eine Entscheidung zwischen den beiden Positionen kann jedenfalls nicht mit dem Argument erfolgen, bei einer Bindung an das BDSG sei die Qualifizierung als sonstige Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG mangels Anwendungsbereichs sinnlos.

So aber Wolff/Brink-Bäcker § 4 Rn. 14

Wie eben ausgeführt, bliebe noch genügend Raum für eine Konkretisierung und Anpassung an die betrieblichen Verhältnisse – von einer Verbesserung des BDSG-Standards ganz abgesehen. Dennoch liegt in der Bemerkung ein berechtigter Kern: Aus systematischen Gründen erschiene es wenig stimmig, wenn das BDSG auf der einen Seite „andere Rechtsvorschriften" ausdrücklich als Ermächtigungen zur Datenverarbeitung zulassen, dann aber eine Bindung an alle seine anderen Tatbestände vorschreiben würde. Mit Recht hat deshalb das BAG darauf verwiesen, die Betriebsvereinbarungen müssten zwar nicht dem BDSG, wohl aber „grundgesetzlichen Wertungen, zwingendem Gesetzesrecht und den allgemeinen Grundsätzen des Arbeitsrechts" Rechnung tragen.

BAG AP Nr. 15 zu § 87 BetrVG 1972 Überwachung

Inzwischen werden die „grundgesetzlichen Wertungen" konkreter gefasst; insbesondere muss das informationelle Selbstbestimmungsrecht der Betroffenen beachtet werden.

BAG NZA 2013, 1433, auch zum Folgenden

Dabei sind die Betriebsparteen an das Verhältnismäßigkeitsprinzip gebunden; der Eingriff in das informationelle Selbstbestimmungsrecht muss geeignet, erforderlich und verhältnismäßig im engeren Sinne sein. Letzteres bedeutet, dass die Schwere des Eingriffs bei einer Gesamtbetrachtung nicht außer Verhältnis zum Gewicht der ihn rechtfertigenden Gründe stehen darf; zwischen den Belangen beider Seiten muss eine Abwägung stattfinden.

Dazu Wybitul NZA 2014, 225 ff.

Diese Grenzen bedeuten, dass die Betriebsparteien auch auf der Grundlage der zweiten Position und der Rechtsprechung kaum mehr Spielraum haben als bei der Anwendung des BDSG; von daher minimieren sich die Unterschiede zwischen beiden Positionen.

So auch Gola/Schomerus § 4 Rn 10a; Forgó/Helfrich/Schneider-Hanloser Teil IV Kap. 1 Rn. 18

Ob die Überprüfung am Maßstab des informationellen Selbstbestimmungsrechts dabei generell „um einige Pegelstriche großzügiger“ sein wird,

So Forgó/Helfrich/Schneider-Hanloser Teil IV Kap. 1 Rn. 18 unter Berufung auf Thüsing RDV 2010, 147, 148

ist durchaus zu bezweifeln. In Bezug auf die hier zur Erörterung stehende konzerninterne Datenübermittlung vertritt allerdings eine ganze Reihe von Autoren den Standpunkt, eine Konzernbetriebsvereinbarung könne insoweit eine zureichende Rechtsgrundlage sein.

Auernhammer-Forst, § 32 Rn. 109; Weth/Herberger/Wächter-Schöttle Teil C III Rn. 55. Vgl. auch Taeger/Gabel-Taeger § 4 Rn. 44

Dem entspricht die Rechtsprechung des BAG, das die Legalisierung einer konzerninternen Datenübermittlung durch Konzernbetriebsvereinbarung gleichfalls nicht beanstandete.

BAG 20. 12. 1995 – 7 ABR 8/95 – NZA 1996, 945

Dies bedeutet allerdings nicht, dass die Natur und „Sensibilität“ der Daten keine Rolle spielen würde und das Arbeitgeberunternehmen alle Personaldaten unterschiedslos an andere Konzernunternehmen weitergeben könnte, sobald nur eine Konzernbetriebsvereinbarung existiert. Vielmehr muss auch hier zwischen dem legitimen Informationsinteresse der Arbeitsgeberseite und dem ebenso legitimen Abschirmungsinteresse des Beschäftigten abgewogen werden. Beispiele hierfür bietet das Personalaktenrecht innerhalb desselben Unternehmens.

In der BAG-Entscheidung vom 15. Juli 1987 (NZA 1988, 55) ging es um die Frage, ob Gutachten und Vermerke über den Gesundheitszustand und die Persönlichkeitsstruktur des Arbeitnehmers in der Personalakte bleiben mussten, so dass sie jeder Sachbearbeiter zu Gesicht bekam, der über einen normalen Urlaubsantrag zu befinden hatte. Das BAG meinte, diese Unterlagen müssten ggf. separat aufbewahrt und nur solchen Sachbearbeitern zugänglich gemacht werden, die gerade auf sie zurückgreifen müssten. Der Kreis der mit Personalakten befassten Personen müsse möglichst eng gezogen werden, was auch der 9. Senat in seiner Entscheidung vom 12. 9. 2006 (BAG NZA 2007, 270) bestätigte.

Wenn schon im Rahmen desselben Unternehmens insoweit zu differenzieren ist, muss dies erst recht bei einer Übermittlung an ein anderes oder gar an alle Konzernunternehmen gelten. Letzteres ist ein sehr viel weitergehender Eingriff in die Persönlichkeitssphäre als eine „großzügige“ Zugriffsregelung in der Personalabteilung, da der Kreis der mit den übermittelten Daten befassten Personen sehr viel größer und aus der Sicht des Einzelnen auch nicht wirklich kontrollierbar ist. Von daher ist immer zu fragen, welche Zwecke mit einer Übermittlung verfolgt werden und wie sehr der Einzelne dadurch betroffen ist.

7. Übermittlung sensitiver Daten nach § 3 Abs. 9 BDSG

Die hier erörterten Rechtsgrundlagen für die konzerninterne Datenübermittlung finden keine Anwendung auf die sog. sensitiven Daten nach § 3 Abs. 9 BDSG. Diese genießen einen Sonderschutz und unterliegen spezifischen Vorschriften, die in § 28 Abs. 6 bis 9 BDSG niedergelegt sind. § 32 Abs. 1 Satz 1 hat insoweit keinen Vorrang.

Plath-Stamer/Kuhnke § 32 Rn. 9; Däubler, Gläserne Belegschaften? Rn. 186a; Wolff/Brink-Riesenhuber § 32 Rn. 30; Taeger/Gabel-Zöll § 32 Rn. 11

Erfasst sind Angaben über die rassische und ethnische Herkunft eines Menschen, wozu auch die Hautfarbe und die Zugehörigkeit zu einer nationalen Minderheit gehören.

Bergmann/Möhrle/Herb, § 3 Rn. 168; Plath-Plath/Schreiber § 3 Rn. 79

Erfasst sind weiter politische Meinungen, was auch die Teilnahme an einer Demonstration sowie die Mitgliedschaft in einer Partei umfasst. Gleichgestellt sind religiöse oder philosophische Überzeugungen, wobei die Mitgliedschaft in Kirchen und bestimmten Vereinigungen sowie entsprechende Aktivitäten gleichfalls einbezogen sind.

Taeger/Gabel-Buchner § 3 Rn. 59

Eine Aussage „X isst keine Schweinefleisch“ stellt im Regelfall eine entsprechende Kennzeichnung dar. Auch atheistische Überzeugungen und Betätigungen sind geschützt.

Bergmann/Möhrle/Herb § 3 Rn. 169; Simitis-Simitis § 3 Rn. 262

Die gleichfalls einbezogene Gewerkschaftszugehörigkeit umfasst auch gewerkschaftliche Aktivitäten sowie das Innehaben bestimmter Funktionen und die Arbeit für gewerkschaftseigene Stiftungen.

Alle diese Angaben dürfen im Regelfall vom Arbeitgeber von vorne herein gar nicht gespeichert und verarbeitet werden. Anders verhält es sich jedoch mit den ebenfalls von § 3 Abs. 9 BDSG erfassten Gesundheitsdaten. Ihrer Verarbeitung kommt große praktische Bedeutung zu. Erfasst sind nicht nur positive („sehr belastbar“) und negative Aussagen („häufig krank“) über den aktuellen Gesundheitszustand, sondern auch Umstände, die wie die Einnahme von Medikamenten oder ein Arztbesuch entsprechende Rückschlüsse zulassen. Einbezogen sind etwa die Abhängigkeit von Drogen, Medikamenten oder Alkohol. Auch Informationen über frühere Erkrankungen sind geschützt.

Nach 28 Abs. 6 Satz 1 BDSG ist die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten insbesondere dann zulässig, wenn der Betroffene eingewilligt hat. Nach § 4a Abs. 3 BDSG muss sich diese Einwilligung allerdings ausdrücklich auf die in Frage stehenden sensitiven Daten beziehen. Da die Einwilligung im Arbeitsverhältnis normalerweise schriftlich erfolgt,

Däubler, Gläserne Belegschaften? Rn. 146

müssen die sensitiven Daten im Text der Erklärung benannt sein.

Ebenso Gola RDV 2001, 126

Außerdem muss der Betroffene bei der Belehrung m. E. nicht nur über die Daten und ihre geplante Verarbeitung als solche, sondern auch darüber informiert werden, dass es sich um besonders geschützte Angaben handelt, die ohne seine Einwilligung nur in engem Rahmen genutzt werden könnten. Ein Hinweis darauf gehört zu den „Konsequenzen der Verweigerung“, die § 4a Abs.1 Satz 2 BDSG für den Regelfall ausdrücklich benannt haben möchte.

Liegt keine Einwilligung vor, so kommt nur eine Übermittlung nach § 38 Abs. 6 Nr. 3 BDSG in Betracht; die anderen Tatbestände (§ 28 Abs. 6 Nr. 1, 2 und 4) sind nicht einschlägig. Danach ist die Erhebung, Verarbeitung und Nutzung sensitiver Daten dann zulässig, wenn dies zur „Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.“ Weiter wird verlangt, dass kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung überwiegt.

„Rechtliche Ansprüche“ der verantwortlichen Stelle, d. h. des Arbeitgebers umfassen auch künftige Ansprüche wie die auf eine vertragsgemäße Arbeitsleistung. Mit der Ausübung und Geltendmachung ist nicht nur der Weg zu den Gerichten, sondern auch ein außergerichtliches Vorgehen gemeint.

Klug RDV 2001, 273; Simitis-Simitis § 28 Rn. 305

Soweit es jedoch nicht um die Geltendmachung oder die Abwehr von Ansprüchen, sondern beispielsweise um die Nachwuchsförderung geht, kann § 28 Abs. 6 Nr. 3 BDSG schon nach seinem Wortlaut nicht eingreifen. Würde man jede vertragliche Beziehung mit Rücksicht darauf genügen lassen, dass aus dieser ja irgendwann ein Anspruch entstehen könnte, so wäre der Unterschied zu § 28 Abs. 1 Satz 1 Nr. 1 BDSG eingeebnet; der Sonderschutz sensibler Daten hätte keinen realen Inhalt mehr. Es mag zwar zutreffen, dass der Arbeitgeber vor der Einstellung sich über den Gesundheitszustand des Bewerbers erkundigen, insbesondere ihn erfragen darf,

Simitis-Simitis § 28 Rn. 306; ihm zustimmend Auernhammer-Kramer, § 28 Rn. 151

doch kann dies nicht dazu führen, dass Gesundheitsdaten wie andere behandelt werden und beispielsweise bei einer Funktionsübertragung quasi-automatisch mit übertragen werden können.

So aber Gola/Wronka, Rn. 820

Ist in einem Konzern beispielsweise die Rechtsverfolgung und die Abwehr von Ansprüchen bei einer zentralen Rechtsabteilung konzentriert, so können dieser bei Bedarf auch Gesundheitsdaten übermittelt werden. Im Rahmen von Talent Management und Vergütungsstrukturen ist dies nicht zu rechtfertigen.

Die auf den Konzernbetriebsrat bezogenen Ausführungen gelten in gleicher Weise für eine Abmachung, die von einem Konzernsprecherausschuss nach §§ 21 ff. SprAG mit der Arbeitgeberseite vereinbart wurde. Voraussetzung ist allerdings nach § 28 Abs. 2 Satz 1 SprAG, dass beide Seiten über die unmittelbare und zwingende Wirkung des Vereinbarten einig sind. Nur dann ist eine Gleichstellung mit den Normenverträgen im Rahmen der Betriebsverfassung möglich. Für die Arbeitgeberseite hat der Abschluss einer solchen Abmachung den Vorteil, auf diese Weise eine eindeutige Rechtsgrundlage für die konzerninterne Übermittlung zu erhalten.

II. Konzerninterne Datenübermittlung ins Ausland

1. EU-Ausland und sichere Drittstaaten

Nach § 4b BDSG gelten für die Übermittlung von Daten in einen andern EU-Mitgliedstaat, in einen EWR-Staat und an Organe und Einrichtungen der EU dieselben Grundsätze wie im Inland. Das EU- und das EWR-Territorium gelten datenschutzrechtlich als Inland. Konsequenterweise sieht deshalb § 3 Abs. 8 Satz 2 BDSG anders als das frühere Recht insoweit auch eine Auftragsdatenverarbeitung über die Grenze vor.

Die Gleichstellung schließt nicht aus, dass sich bei der praktischen Handhabung Unterschiede zu rein innerstaatlichen Sachverhalten ergeben. So kann es etwa eine unbillige Benachteiligung des einzelnen Arbeitnehmers darstellen, wenn die Verarbeitung seiner Daten an einem Ort erfolgt, der für ihn mit zumutbarem Aufwand nicht erreichbar ist und wo er Auskunftsersuchen in einer fremden Sprache abfassen müsste. Auch die Auskunftsrechte des Betriebsrates und des Unternehmenssprecherausschusses sind in Gefahr, gegenüber Vorgängen in ausländischen Konzerngesellschaften zu versagen. Nicht die Existenz einer (politischen) Grenze, wohl aber andere Erschwernisse können datenschutzrechtliche Relevanz gewinnen. Inwieweit dies im vorliegenden Zusammenhang von Bedeutung ist, kann erst mit Zusammenhang mit den verbindlichen Unternehmensregeln, den binding corporate rules (oben A III), erörtert und beurteilt werden.

Dieselben Grundsätze gelten nach § 4b Abs. 2 Satz 1 BDSG für die Übermittlung in ein Drittland, das über ein „angemessenes“ Datenschutzniveau verfügt. Eine Ausnahme gilt allerdings insoweit, als hier keine Auftragsdatenverarbeitung möglich ist: Auch wenn ein in einem Drittland eingeschaltetes Unternehmen in Bezug auf die übermittelten Daten voll den Weisungen des in der EU ansässigen Unternehmens unterliegt, besteht rechtlich ein Fall von Datenübermittlung.

An sich ist es Aufgabe der verantwortlichen Stelle, die Gleichwertigkeit des ausländischen Datenschutzrechts zu beurteilen. Dies könnte jedoch zu einem hohen Maß an Rechtsunsicherheit führen, da über die „Angemessenheit“ unterschiedliche Ansichten bestehen können. Art. 25 Abs. 6 der EU-Datenschutzrichtlinie ermächtigt deshalb die

Kommission, mit Bindung für alle Instanzen der Mitgliedstaaten über die Angemessenheit des Datenschutzniveaus zu entscheiden. Dies ist u. a. in Bezug auf Argentinien, Kanada,, Australien und Israel sowie Uruguay und die Schweiz geschehen.

2. Drittstaaten ohne angemessenes Datenschutzniveau

Soweit – wie bei der Mehrzahl aller Staaten – keine positive Kommissionsentscheidung über ein angemessenes Datenschutzniveau vorliegt, greift § 4c BDSG ein. Dabei ist zwischen dem „Normalfall“ und der Sondersituation im Verhältnis zu den USA zu unterscheiden.

a.) Der Normalfall

Die Übermittlung kann nach § 4c Abs. 1 Satz 1 Nr. 1 BDSG durch die Einwilligung des Betroffenen gerechtfertigt sein. Dies lässt sich bei weltweiten NGOs wie Greenpeace unschwer praktizieren, doch passt diese Lösung nicht auf das Beschäftigungsverhältnis.

So auch die Stellungnahme der hessischen Landesregierung, RDV 2002, 38

Ein solcher „Blankoscheck“, der offen lässt, was mit den Arbeitnehmerdaten in dem Land ohne (angemessenes) Datenschutzrecht geschieht, würde den Beschäftigten unangemessen benachteiligen und auch nicht dem Bestimmtheitsgebot Rechnung tragen. Weiter setzt eine wirksame Einwilligung eine vorherige Aufklärung über die spezifischen Risiken voraus.

Soweit ein Arbeitnehmer in das betreffende Drittland entsandt wird, lässt sich die Datenübermittlung im Rahmen des Notwendigen auf § 4c Abs. 1 Satz 1 Nr. 2 BDSG stützen, wonach sie zulässig ist, wenn sie der Erfüllung eines Vertrages zwischen dem Betroffenem (Arbeitnehmer) und der verantwortlichen Stelle (Arbeitgeber) dient.

Ebenso die hessische Landesregierung RDV 2002, 38

In anderen Fällen lässt sich ein gleichwertiger, zumindest angemessener Schutz des informationellen Selbstbestimmungsrechts dadurch sicherstellen, dass die verantwortliche

Stelle mit dem ausländischen Übermittlungsempfänger einen Vertrag schließt, der entsprechende Schutzvorkehrungen beinhaltet. Die EU-Kommission stellt insoweit Musterverträge bereit. Werden sie übernommen, bedarf es nicht noch zusätzlich einer behördlichen Genehmigung für den Datentransfer. Werden sie nicht übernommen, bleibt im Regelfall die Genehmigungspflicht bestehen.

In multinationalen Konzernen stellt sich das Problem, wer von verschiedenen Niederlassungen innerhalb der EU den Vertrag schließt. Die Aufsichtsbehörden stellen darauf ab, wo die Entscheidung für oder gegen die Übermittlung fällt; ist hierfür die Konzernspitze im Inland zuständig, ist der Vertragsschluss allein ihre Sache.

Hillenbrand-Beck RDV 2007, 232

Dasselbe gilt dann, wenn eine inländische Tochtergesellschaft insoweit eigene Entscheidungsbefugnisse hat.

Bei multinationalen Konzernen steht ein zweiter Weg zur Verfügung, um den notwendigen Persönlichkeitsschutz sicherzustellen. Möglich sind hier „verbindliche Unternehmensregelungen“, über die das BDSG keine näheren Angaben macht, die jedoch Gegenstand verschiedener Dokumente der Arbeitsgrippe nach Art. 29 Datenschutz-Richtlinie sind.

Insbesondere WP 74 (=Working paper Nr. 74), abrufbar unter http://ec.europe.ez/justice-home/fsj/privacy/docs/wpdocs/2003/wp74-de.pdf

Fest steht zunächst, dass es nicht ausreichen kann, wenn die Konzernspitze oder die einzelnen beteiligten Unternehmen „Wohlverhaltenserklärungen“ abgeben, wie sie sich häufig unter dem Stichwort des „Code of Conduct“ in der Praxis finden. Ihnen fehlt ersichtlich der verbindliche Charakter, von dem § 4b Abs. 2 Satz 1 BDSG ausgeht.

Für notwendige rechtliche Verbindlichkeit auch Filip ZD 2013, 51, 57; Heil DuD 2009, 229; Plath – v. d. Bussche § 4c Rn. 40; Scheja, Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank: eine Untersuchung unter besonderer Berücksichtigung der §§ 4b, 4c BDSG, Baden-Baden 2006, S. 246; Weniger,

Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen, Hamburg 2005, S. 504 f.; Wolff/Brink-Schantz § 4c Rn. 60

Der Terminologie der Art. 29 – Gruppe nach muss Verbindlichkeit nach innen (etwa durch Weisungen, den „Kodex" korrekt zu befolgen) wie nach außen (etwa durch Einräumung von einklagbaren Ansprüchen an die Betroffenen) bestehen. Fehlt es daran, kann die Abmachung keine rechtfertigende Wirkung entfalten; sie bleibt wirkungslos. Da die „Unternehmensregelungen" ein Äquivalent zu vertraglichen Bindungen zwischen von einander unabhängigen Unternehmen sind, müssen sie auch ein vergleichbares Maß an Datenschutz gewährleisten.

Filip ZD 2013, 51, 57; C. Schröder, Die Haftung für Versröße gegen Privacy Policies und Codes of Conduct nach US-amerikanischem und deutschem Recht: Zugleich ein Beitrag zu Rechtsnatur von Datenschutzerklärungen, Verhaltensregeln gem. § 38a BDSG und Unternehmensregelungen gem. § 4c Abs. 2 BDSG, Baden-Baden 2007, S. 208 ff. S. auch Taeger/Gabel-Gabel § 4c n. 29.

Liegt eine verbindliche Unternehmensregelung vor, bedarf es gleichwohl einer staatlichen Genehmigung. Ein „Musterkodex" analog den Standardverträgen der EU-Kommission existiert bislang nicht, doch stellen diese eine wichtige Orientierungsgröße dar.

Achim Büllesbach, Transnationalität und Datenschutz. Die Verbindlichkeit von Unternehmensregelungen, Baden-Baden 2008, S. 176 ff.; Räther DuD 2005, 462; Weichert DuD 2010, 679, 687; s. auch Scheja, a. a. O., . 261 ff.

Die Art. 29-Gruppe hat mittlerweile auch Anleitungen erarbeitet, wie bindende Unternehmensregeln beschaffen sein müssen, wenn eine Auftragsdatenverarbeitung mit einem in einem Drittstaat befindlichen Auftragnehmer stattfinden soll.

Filip ZD 2013, 51, 58 f.

Dies ist insbesondere für das cloud computing von Bedeutung.

Enthalten die verbindlichen Unternehmensregeln lediglich pauschale Regeln in Bezug auf jede Art von Daten, so bleibt das Genehmigungserfordernis im konkreten Fall bestehen, da § 4c Abs. 1 Satz 2 BDSG nur „einzelne Übermittlungen“ und „bestimmte Arten von Übermittlungen“ für genehmigungsfähig erklärt; nur insoweit kommt die einheitliche Unternehmensregelung ins Spiel. Geht es einmal um die Übermittlung von Entgeltdaten, sind aber im nächsten Fall Daten zur Karriereplanung erfasst, so ist beide Male eine staatliche Genehmigung erforderlich. Selbst wenn die verbindliche Unternehmensregelung als solche von der Aufsichtsbehörde genehmigt worden ist, ändert sich daran angesichts des eindeutigen Wortlauts des § 4c Abs. 1 Satz 1 nichts.

Plath - v. d. Bussche § 4c Rn. 41; Wolff/Brink-Schantz § 4c Rn. 57

Die Existenz verbindlicher Unternehmensregeln erleichtert allerdings entscheidend die Erteilung der Genehmigung, da typischerweise keine Abweichung von der für den Normalfall vorgesehenen Regelung vorliegen wird.

b.) Datenübermittlung in die USA

Gerade im Arbeitsrecht weisen die USA kein Datenschutzniveau auf, das man nach unseren Maßstäben als angemessen ansehen kann.

Wilske CR 1993, 297; Däubler CR 1999, 53; zu den konzeptionellen Unterschieden s. Buchner, Informationelles Selbstbestimmungsrecht, a. a. O., S. 7 ff.; Weichert RDV 2010, 113

Um den Handelverkehr nicht unnötig zu belasten, ist zwischen der EU-Kommission und dem US-Handelsministerium eine Abmachung getroffen worden,. Danach sind Unternehmen aus den USA dann grundsätzlich taugliche Datenempfänger, wenn sie sich den Grundsätzen über den sog. sicheren Hafen (safe harbor principles) angeschlossen haben. Über ihre Einhaltung wacht die Federal Trade Commission, doch wird sie nur auf Beschwerde hin aktiv.

Einzelheiten bei Klug RDV 2000, 212. Die safe harbor principles sind abrufbar unter www.export.gov/safeharbor

In der EU ist Rechtsgrundlage eine Entscheidung der EG-Kommission vom 26. Juli 2000 (ABl v. 25. 8. 2000 Nr. L 215/7 ff.), die seit November 2000 praktiziert werden konnte. Die Lösung ist im Ansatz intelligent, da sie auf amerikanische Souveränitätsvorstellungen Rücksicht nimmt, gleichzeitig aber den Anspruch des europäischen Datenschutzrechts aufrechterhält.

Seit dem Abschluss der Vereinbarung haben sich jedoch zahlreiche negative Erfahrungen ergeben; Unternehmen unterstellen sich nur formal den Safe-Harbor-Principles, ohne den dort festgelegten Anforderungen in der Realität zu entsprechen. Kontrollen finden selten statt. Bei Verstößen sind die Sanktionen außerordentlich bescheiden. Lediglich bei einem Verdacht unlauteren oder betrügerischen Verhaltens wird ein Unternehmen von der Liste gestrichen, doch muss es kein Bußgeld befürchten.

> Dazu Marnau/Schlehahn DuD 2011, 311, 314; kritisch weiter Simitis-Simitis § 4b Rn. 70 ff.; Tinnefeld/Buchner/Petri, Einführung, a. a. O., S. 266; HK-ArbR-Hilbrans, a. a. O., §§ 4b, 4c Rn. 3.

Der Düsseldorfer Kreis der Aufsichtsbehörden hat deshalb im April 2010 beschlossen, von den deutschen „Datenexporteuren“ zusätzliche Nachweise zu verlangen, wonach der US-Partner den Safe-Harbor-Principles effektiv nachkommt, insbesondere auch seine Informationspflichten gegenüber den Betroffenen erfüllt.

> Einzelheiten bei Marnau/Schlehahn DuD 2011, 311, 315; Auernhammer-Thomale § 4b Rn. 17.

Die Aufdeckung der NSA-Aktivitäten hat die Konferenz der Datenschutzbeauftragten zu einer gemeinsamen Erklärung veranlasst, wonach keine Genehmigungen mehr erteilt werden, solange der unbeschränkte Zugriff ausländischer Nachrichtendienste auf personenbezogene Daten besteht. Außerdem wird die EU-Kommission aufgefordert, ihre Entscheidung zugunsten der Safe-Harbor-Principles zu suspendieren.

> Die Presseerklärung vom 24. 7. 2013 ist nachlesbar unter http://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.9283.de

Heftige Kritik an der US-Politik bei Spies ZD 2013, 535 ff. Negativprognose in Bezug auf die Zukunft der Safe-Harbor-Principles bei Forgó/Helfrich/Schneider-Schneider Teil II Kap. 4 Rn. 50.

Soweit sich ein Unternehmen den Safe-Harbor-Prinzipien nicht anschließen will oder mangels Zuständigkeit der Federal Trade Commission nicht anschließen kann, gelten die Regeln, die gegenüber sonstigen Drittstaaten mit nicht angemessenem Datenschutzniveau praktiziert werden.

Gerhold/Heil, DuD 2001, 378

Die Übermittlung personenbezogener Daten in die USA ist seit einer Reihe von Jahren mit einer weiteren Hypothek versehen: Aufgrund des Patriot Act ist jederzeit ein staatlicher Zugriff auf die Daten möglich.

Zum Inhalt des Patriot Act s. die kurze Zusammenfassung bei Voigt/Klein ZD 2013, 16 f.

Zwar muss sich der Zugriff inhaltlich mit dem Zweck der Terrorismusbekämpfung rechtfertigen lassen, doch ist faktisch so gut wie keine Kontrolle möglich, ob sich diese Begründung effektiv auf Tatsachen stützen kann oder ob sie nur vorgeschoben war. Dies nicht zuletzt deshalb, weil das US-Unternehmen, auf dessen Daten zugegriffen wurde, in der Regel verpflichtet wird, über diesen Tatbestand Stillschweigen zu bewahren. Weil Betroffene nichts erfahren, können sie sich auch nicht zur Wehr setzen. Für europäische Firmen besteht unter diesen Umständen das Risiko, dass Betriebs- und Geschäftsgeheimnisse der US-amerikanischen Konkurrenz bekannt werden können. Um dies zu vermeiden, bieten bestimmte Firmen im Rahmen des Cloud computing nur noch Speicherplatz in Europa an. Auch für Arbeitnehmer ist der heimliche und unkontrollierte Zugriff auf ihre Daten nicht zumutbar.

III. Konsequenzen für die Beschäftigten von SADG

Sanofi-Aventis verfügt über ein ausgebautes System des Datenschutzes, das sich in dieser Ausprägung keineswegs bei allen vergleichbaren Konzernen findet. Die geschaffenen Vertragswerke, über die in Teil A berichtet wurde, verdienen in hohem Maße Anerkennung. Dennoch ergeben sich im Zusammenhang mit der Einführung von Workday eine Reihe von Bedenken, die sich aber nach Einschätzung des Gutachters im Geiste der Kooperation lösen lassen.

1. Das Problem der Rechtsgrundlage

Die Arbeit mit Workday führt unbestrittenermaßen dazu, dass die eingegebenen Daten von zahlreichen Personen im Ausland, sogar in Drittstaaten ohne angemessenes Datenschutzniveau abgerufen und eingesehen werden können. Dies stellt eine Übermittlung nach § 3 Abs. 4 Nr. 3 Buchstabe b BDSG dar. Werden Daten an andere Konzernunternehmen übermittelt, bedarf es dazu – wie unter C I ausgeführt – einer Rechtsgrundlage.

§ 32 Abs. 1 Satz 1 BDSG wird in vielen Fällen eingreifen können, da die Arbeitsverhältnisse einen konzerndimensionalen Charakter besitzen, also kraft Arbeitsvertrags auch ein Einsatz in einem andern Konzernunternehmen in Betracht kommt. Dies gilt insbesondere auch für Leitende Angestellte. Allerdings wird es selbst in dieser Beschäftigtengruppe eine mehr oder weniger große Zahl an Personen geben, nach deren Arbeitsvertrag nur eine Tätigkeit für den unmittelbaren Arbeitgeber, d. h. in Deutschland in Betracht kommt. Im Einzelnen ist dies oben unter C I 1 ausgeführt.

Für diese Gruppe muss eine der anderen Rechtsgrundlagen herangezogen werden. § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist nach überwiegender Auffassung in der Literatur auf Beschäftigtendaten nicht anwendbar. Schließt man sich der Minderheitenposition an, so stellt sich das Problem der Interessenabwägung. In der Literatur wird von beachtlichen Stimmen verlangt, dass der Vertragsarbeitgeber weiter entscheidender Anspruchpartner der einzelnen Beschäftigten sein muss, was hier durchaus der Fall ist. Hinzu kommen muss aber, dass der Arbeitnehmer durch die Übermittlung in seiner Rechtsstellung nicht wesentlich beeinträchtigt wird, dass seine Rechtsstellung grundsätzlich dieselbe bleibt; der

Datenempfänger dürfe keine Befugnisse bekommen, die der Arbeitgeber nicht habe (oben C I 2 b). Genau dies ist aber der Fall, wenn bei „Leistung und Vergütung“ und bei „Talentförderung und Nachfolgeplanung“ der Kreis der Beschäftigten drastisch erweitert wird, die in eine vergleichende Betrachtung einbezogen werden können. Die Rechte der Arbeitgeberseite werden – in durchaus verständlicher und nachvollziehbarer Weise - erweitert, ohne dass dem eine Verbesserung der Rechtsstellung des Beschäftigten gegenüber stehen würde.

Das Mittel der Einwilligung wurde in Bezug auf das System als Ganzes nicht eingesetzt, weil die Arbeitgeberseite davon ausging, dass bestimmte Angaben obligatorisch seien. Lediglich bei bestimmten Angaben kommt es auf die Freiwilligkeit an, was jedoch spezifische Probleme aufwirft, die im Folgenden behandelt werden (unten 2). Die Auftragsdatenverarbeitung mag im Verhältnis zwischen SAG und Workday vorliegen, doch geht die konzerninterne Datenübermittlung weit über die Erledigung eines Auftrags hinaus, weil auch Entscheidungsbefugnisse bei anderen Konzernunternehmen entstehen. Davon gehen ersichtlich auch die „Binding Corporate Rules“ aus, die bei einer Beschränkung auf die Auftragsdatenverarbeitung weitgehend überflüssig wären. Auch das Datenschutzabkommen zwischen SADG und SAG (oben A II) geht nicht davon aus, dass SADG ausschließlich Weisungen an SAG erteilt.

Was als Rechtsgrundlage bleibt, ist eine (Konzern-)Betriebsvereinbarung, die als vorläufige für alle dem BetrVG unterliegenden Arbeitnehmer vorliegt. Für die Leitenden Angestellten ist es bisher trotz verschiedener Angebote des Unternehmenssprecherausschusses noch nicht zu einem Abschluss gekommen. Insoweit fehlt es bei ihnen an einer umfassenden Rechtsgrundlage, da § 32 Abs. 1 Satz 1 BDSG – wie ausgeführt – nicht alle Beschäftigten dieser Gruppe erfassen kann.

Ausgenommen von der Übermittlung sind krankheitsbedingte Fehlzeiten, da es sich insoweit um sensitive Daten im Sinne des § 3 Abs. 9 BDSG handelt und die spezifischen Voraussetzungen des § 26 Abs. 6 bis 9 BDSG nicht vorliegen.

Soweit es zu einem Abschluss kommt, ist selbstredend den weiteren hier genannten Gesichtspunkten Rechnung zu tragen.

2. Die Probleme der Einwilligung

Bei einem Teil der sog. Talentdaten steht es dem Einzelnen frei, ob er Angaben machen will oder nicht. Diese unbestrittene Tatsache ist allerdings nicht immer mit der nötigen Deutlichkeit zum Ausdruck gebracht worden; vielmehr konnte der Eindruck entstehen, dass sich alle Fragen auf Pflichtangaben beziehen. Dies wird an einem an zahlreiche Beschäftigte gerichteten E-Mail deutlich, wo es wörtlich heißt:

„Liebe Mitarbeiterinnen und Mitarbeiter,
wie Ihnen bekannt ist, müssen die Eingaben in Workday zum Talent Review bis Ende Juni abgeschlossen sein.
Ihre Eingaben fehlen noch und müssen dringend ergänzt werden.
Bitte holen Sie dies umgehend nach und nehmen Sie diesbezüglich umgehend Kontakt mit Ihrer/m Vorgesetzten auf.
Bitte denken Sie auch daran, dass im Rahmen des Genehmigungsprozesses nach ihrer Eingabe weitere Schritte u. a. durch Ihre/n Vorgesetzte/n erforderlich sind.
Grüße“

Die Dateneingabe wird hier als sehr dringlich dargestellt; dass bestimmte Angaben gar nicht erforderlich sind, wird mit keinem Wort erwähnt. Inhaltlich entsteht der Eindruck einer „Ermahnung“, die darauf gerichtet ist, die bisher unterbliebene Pflichterfüllung möglichst schnell nachzuholen.

Dazu kam, dass in der Eingabemaske – so wird berichtet – die Felder nicht besonders gekennzeichnet waren, die sich auf freiwillige Angaben bezogen.

Damit ist eine Situation gegeben, die die Datenerhebung insgesamt als fehlerbehaftet erscheinen lässt, weil die Arbeitnehmer von falschen Voraussetzungen ausgehen mussten. Eine solche Form der Datenerhebung ist nicht „erforderlich“ im Sinne des § 32 Abs. 1 Satz 1 BDSG und auch nicht von der vorläufigen Betriebsvereinbarung gedeckt. Inhaltlich verstößt sie gegen Treu und Glauben. Die unzulässige Erhebung gibt den Betroffenen nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG ein Recht auf Löschung, da ihre Speicherung unzulässig war.

Vor einer erneuten Datenerhebung sollte zunächst auch gegenüber den Leitenden Angestellten für eine ausreichende Rechtsgrundlage gesorgt werden. Anschließend ist bei der Datenerfassung deutlich zwischen obligatorischen und freiwilligen Angaben zu unterscheiden.

Außerdem ist § 4 Abs.3 Satz 1 BDSG zu beachten, wonach die Betroffenen u. a. davon in Kenntnis gesetzt werden müssen, welche Zwecke mit der Erhebung, Verarbeitung und Nutzung der Daten verfolgt werden. Die Aushändigung eines „Benutzerhandbuchs", das den Einzelnen in die Lage versetzt, eine Reihe von Daten einzugeben und zu korrigieren, ist hierfür nicht ausreichend. Vielmehr muss explizit darauf hingewiesen werden, welcher Gebrauch beispielsweise von den eingegebenen Daten gemacht werden kann, inwieweit sie bei Personalentscheidungen, insbesondere bei Beförderungen und Versetzungen, berücksichtigt werden.

Was den freiwilligen Teil betrifft, so ist der Betroffene nach § 4a Abs. 1 Satz 2 BDSG gleichfalls auf den vorgesehenen Verwendungszweck hinzuweisen. Dazu muss nach derselben Vorschrift ein Hinweis darauf kommen, welche Folgen die Nichterteilung der Einwilligung, d. h. die Verweigerung der Angaben haben kann. Davon war bisher in den verfügbaren Unterlagen nicht die Rede, doch könnte eine unfassende Aufklärung für das Verhalten der Beschäftigten von erheblicher Bedeutung sein.

Weitere Anforderungen an eine korrekte und damit wirksame Einwilligung sind oben unter C I 4 dargestellt.

3. Löschung von Eintragungen

Im „Handbuch Talent" findet sich auf S. 5 und auf S. 8 die mit „Achtung!" hervorgehobene Feststellung, wer Entwicklungsfelder außerhalb des entwicklungsorientierten Talent Review im Profil anlege, könne diese nicht mehr löschen. Möglich sei lediglich, die Eintragung in den Status „nicht anwendbar" zu versetzen, was dazu führe, dass die Eintragung als durchgestrichene angezeigt würde.

Auch hier stellt sich die Frage, inwieweit eine solche Regelung als „erforderlich" im Sinne des § 32 Abs. 1 Satz 1 BDSG bzw. der Gesamtbetriebsvereinbarung angesehen

werden kann. Soweit es sich – wie hier – um eine freiwillige Angabe handelt, steht dem Betroffenen außerdem ein Widerrufsrecht zu (dazu oben C I 4), dessen Ausübung zur Löschung der fraglichen Eingabe führen muss, weil die weitere Speicherung unzulässig ist und deshalb § 35 Abs. 2 Satz 2 Nr. 1 BDSG eingreift.

Simitis-Simitis § 4a Rn. 103

Davon ganz abgesehen erscheint es als unberechtigter Eingriff in das allgemeine Persönlichkeitsrecht, wenn einem Beschäftigten selbst nach zehn Jahren aufgrund der durchgestrichenen Angabe entgegen gehalten werden kann, was er einmal für (heute lächerlich erscheinende) Pläne hatte. Es sollte daher auch aus diesem Grund bei der Löschung bleiben.

4. Zugriff öffentlicher Stellen in den USA?

Spezifische Probleme ergeben sich aufgrund der Tatsache, dass in den USA aufgrund des Patriot Acts auf zahllose Daten zugegriffen werden kann (näher oben C II 2 b). Dies kann im vorliegenden Zusammenhang einmal Mitarbeiter von SAG betreffen, die regelmäßig von den USA aus tätig sind und die Zugriff auf weite Teile des Systems haben. Zum zweiten kommen auch in den USA ansässige Workday-Mitarbeiter in Betracht, die Zugriff auf die Server in Dublin und Amsterdam haben. Beide Personengruppen können sich einer Anforderung nach dem Patriot Act ausgesetzt sehen.

Ohne Bedeutung ist, dass Workday die Daten mit einem anerkannten Programm verschlüsselt: Es geht nicht darum, einen sowieso illegalen Zugriff auf die Daten während der Übermittlung in die Betrachtung einzubeziehen. Vielmehr geht es allein um die nach US-Recht legale Aufforderung an einen Gebietsansässigen, die ihm zugänglichen Daten zur Verfügung zu stellen und darüber Stillschweigen zu bewahren. Die Möglichkeit eines solchen Zugriffs ist in dem Vertrag mit Workday (oben A I – S. 3) und im Datenschutzvertrag zwischen SADG und SAG (oben A II - S. 5) ausdrücklich angesprochen. Dies bedeutet allerdings nicht, dass er damit zulässig gemacht wäre.

Am 1. Juli 2015 fragte Herr Stöppler namens SADG bei SAG an, wie dort der Umgang mit dem Patriot Act und den mit ihm verbundenen Zugriffsbefugnissen gehandhabt werde.

Die Antwort von Herrn Vibert vom 2. Juli 2015 betont zunächst, dieselbe Frage sei in der Diskussion mit den französischen Gewerkschaften Thema gewesen. Weiter schreibt er:

„Here are the elements that protect Sanofi employees data:

1. Workday servers holding Sanofi employees data are located within the European Union (Dublin and Amsterdam).
2. Workday maintains a Safe Harbor certification which guarantees that they comply with European Union data privacy data protection standards.
3. The contract between Sanofi and Workday and its associated Data Processing Agreement guarantees that Workday employees follow strict data privacy policies and procedures and that they do not access, use, disclose, or transfer customer data unless it is in accordance with a contractual agreement or at the direction of the customer.
4. Workday maintains ISO 27001:2005 certification and is regularly audited (SOC 1 and SOC 2 reports)."

Das eigentliche Problem – der verdeckte Zugriff – ist in dieser Antwort nicht angesprochen. Die Datenerhebung nach dem Patriot Act lässt sich mit europäischen Datenschutzgrundsätzen nicht vereinbaren. Dies einmal deshalb nicht, weil die Eingriffsvoraussetzungen sehr weit formuliert sind und keine reale Möglichkeit besteht, ihr Vorliegen im Einzelfall festzustellen. Dazu kommt, dass der Eingriff als solcher dem Betroffenen nicht zur Kenntnis kommt, so dass er sich dagegen auch nicht zur Wehr setzen kann. Dies verstößt in elementarer Weise gegen den Grundsatz der Datentransparenz.

Die US-Regelung als solche in Frage zu stellen, kann nicht in Betracht kommen. Möglich ist jedoch, das eigene Informationssystem so auszugestalten, dass von den USA aus auf die Server in Dublin und Amsterdam nur insoweit ein Zugriff besteht, als in den USA generierte Daten in Rede stehen. Weitergehende Zugriffe auf Konzernunternehmen in anderen Teilen der Welt müssen ausgeschlossen sein. Für eine solche Lösung spricht nicht nur der Datenschutz der betroffenen Arbeitnehmer. Auch die SAG kann kein Interesse haben, dass beispielsweise von dritter Seite in die Daten des Talent Managements Einsicht genommen wird und bestimmen Leistungsträgern dann ein besonders lukratives Angebot seitens eines US-amerikanischen Konkurrenten gemacht wird. Auch ist denkbar, dass die

Eintragungen Rückschlüsse auf Forschungsschwerpunkte ermöglichen, was wiederum für ein im Wettbewerb mit Sanofi stehendes Unternehmen von erheblichem Nutzen sein könnte.

Die Problematik stellt sich im Übrigen nicht nur für Zugriffe aus den USA. Soweit Sanofi-Beschäftigte in der Volksrepublik China tätig sind und weltweiten Zugriff auf Personaldaten haben, sind vergleichbare Vorgänge denkbar.

Das Personalinformationssystem Workday ist also insoweit zu korrigieren, als in den USA und China Zugriffsrechte auf Daten beschränkt werden, die in dem fraglichen land angefallen sind. Personen mit globaler Zuständigkeit müssten daher ihren Arbeitsplatz in Europa oder einem sicheren Drittstaat haben.

IV. Zusammenfassung

1. Datenübermittlungen im Rahmen des Personalinformationssystems „Workday“ haben die zahlreichen Regeln zu beachten, die innerhalb der Sanofi-Aventis-Groupe gelten. Es handelt es dabei insbesondere um
- das Master Subscription Agreement samt Anhängen,
- das Datenschutzabkommen zwischen der Sanofi-Aventis Deutschland GmbH und der Sanofi-Aventis Groupe Paris,
- die verbindlichen Unternehmensregelungen zum Datenschutz und
- die Gesamtbetriebsvereinbarung zum Personalinformationssystem Workday.
Danach kommt dem Datenschutz ein hohes Stellenwert zu.

2. Die Datenübermittlung zwischen zwei Konzernunternehmen bedarf einer besonderen Rechtsgrundlage, da „verantwortliche Stelle“ im Sinne des deutschen und europäischen Datenschutzrechts das einzelne Konzernunternehmen ist.

3. Als Rechtsgrundlage kommt nach § 32 Abs. 1 Satz 1 BDSG der Arbeitsvertrag in all jenen Fällen in Betracht, in denen das Arbeitsverhältnis auf den Gesamtkonzern bezogen ist. Dies ist bei vielen, aber nicht bei allen Führungskräften der Fall.

4. § 28 Abs. 1 Satz 1 Nr. 2 BDSG kommt nach mehrheitlich in der Literatur vertretener Auffassung neben § 32 nicht zur Anwendung. Sieht man dies mit der Gegenmeinung anders, muss dafür gesorgt werden, dass die Arbeitnehmer möglichst geringe Eingriffe in ihre Persönlichkeitssphäre hinnehmen müssen. Notwendig ist insbesondere, dass sich die Handlungsmöglichkeiten der Arbeitgeberseite nicht wesentlich erweitern und dass die Arbeitnehmer alle Individualrechte auch direkt gegenüber ihrem Arbeitgeber geltend machen können. Dass diese Voraussetzungen gegeben sind, ist bislang nicht dargetan.

5. Die Einwilligung des Arbeitnehmers nach § 4a BDSG und die Auftragsdatenverarbeitung nach § 11 BDSG sind im konkreten Fall keine geeigneten Mittel, um den Datenfluss zu legitimieren.

6. Für alle nicht konzerndimensionalen Arbeitsverträge kommt als sichere Rechtsgrundlage nur eine (Konzern-) Betriebsvereinbarung in Betracht. Dabei muss auch

hier zwischen dem legitimen Informationsinteresse der Arbeitgeberseite und dem ebenso legitimen Abschirmungsinteresse der Beschäftigten abgewogen werden.

7. Sensitive Daten können nur übermittelt werden, soweit die Voraussetzungen des § 28 Abs. 6 BDSG gegeben sind. Dies ist im vorliegenden Fall nicht ersichtlich. Betroffen sind insbesondere Gesundheitsdaten, zu denen auch Angaben über krankheitsbedingte Fehlzeiten gehören.

8. Die beschriebenen Grundsätze gelten nicht nur bei einer Übermittlung im Inland, sondern auch bei einer Übermittlung in einen anderen EU-Mitgliedstaat, in ein EWR-Land und in sog. sichere Drittländer.

9. Bei einer Übermittlung in Drittstaaten ohne angemessenes Datenschutzniveau ist in der Regel eine staatliche Genehmigung erforderlich, die nur erteilt wird, wenn der Persönlichkeitsschutz auf andere Weise sichergestellt ist. Dies geschieht im Fall der Sanofi-Aventis-Groupe durch verbindliche Unternehmensregelungen. Diese müssen sich allerdings auf „einzelne Übermittlungen“ oder „bestimmte Arten von Übermittlungen“ beziehen.

10. Die Datenübermittlung in die USA stößt auf besondere Schwierigkeiten, da der Übermittler sicherstellen muss, dass die Safe-Harbor-Grundsätze vom Datenempfänger auch wirklich eingehalten werden. Außerdem besteht die Gefahr, dass auf der Grundlage des Patriot Act auf bestimmte Daten zugegriffen wird, ohne dass Sanofi oder der Betroffene davon etwas erfahren. Personen, die Zugriff auf Daten in anderen Ländern haben, dürfen daher ihren Arbeitsplatz nicht in den USA haben.

11. Gibt ein Arbeitnehmer Daten in das System „Workday“ ein und hat er dabei die Vorstellung, dazu verpflichtet zu sein, so kann er diese Daten wieder entfernen, wenn ihre Eingabe in Wirklichkeit freiwillig war.

12. Soweit der Arbeitnehmer verlangen kann, dass bestimmte Daten aus dem System entfernt werden, weil er beispielsweise von seinem Widerrufsrecht Gebrauch gemacht hat, so genügt es nicht, dass sie in Zukunft weiter eingesehen werden können, aber als „durchgestrichen“ in Erscheinung treten.

V. Offene Fragen

Eine Reihe von Fragen ist bisher offen geblieben, weil nicht alle in Betracht kommenden Fakten dem Unternehmenssprecherausschuss und dem Gutachter vorliegen. Dabei handelt es sich insbesondere um folgende Bereiche:

1. Im Unternehmen gibt es die Vorstellung, dass mit Rücksicht auf das von Workday betonte Transparenzprinzip „jedermann“ „alle“ Daten der übrigen Mitarbeiter sehen könne. Was trifft davon zu?
- Können Betriebsangehörige gespeicherte Daten aller anderen Mitarbeiter einsehen? Wenn ja, welche? Wer hat beispielsweise Zugriff auf die Angaben im „Talent Management“, insbesondere auf die Eigeneinschätzung und die Beurteilung durch den Vorgesetzten?
- Erstrecken sich Einsichtsrechte anderer Beschäftigter auch auf die Daten leitender Angestellter?
- Welche Mitarbeiterdaten stehen dem Betriebsrat zur Verfügung?
- Gibt es Zugriffsrechte auch von anderen Niederlassungen aus? Sind auch ausländische Konzernunternehmen einbezogen? Welche Daten können hier durch wen eingesehen werden?

Datenschutzrechtlich ist der Erforderlichkeitsgrundsatz nach § 32 Abs. 1 Satz 1 BDSG und der Grundsatz der Datensparsamkeit nach § 3a BDSG zu beachten.

2. Aus den schriftlichen Unterlagen zu Workday ergibt sich nicht, dass ein Unternehmen einzelne Module kaufen kann. Aufgrund der Besprechung vom 23. Juli 2015 besteht jedoch Grund zu der Annahme, dass ähnlich wie bei SAP Module erworben werden können. Trifft dies zu? Wenn ja, welche Module wurden erworben? Wo ist beschrieben, welche Datenverarbeitung mit ihnen möglich ist?

3. Im Rahmen des Talent Management macht das System Workday Vorschläge. Dies kann dazu führen, dass ihnen mehr oder weniger automatisch gefolgt wird, weil sich der Begründungsaufwand minimiert. Ist das System auch in der Lage, die Konsequenzen zu beschreiben, die sich bei einer anderen Entscheidung ergeben würden?
Datenschutzrechtlich geht es darum, der Wertentscheidung des § 6a BDSG Rechnung zu tragen.

4. Können die im System „Workday“ vorgehaltenen Angaben über Vergütung, Leistung, Talent und weitere Punkte dazu führen, dass ein Persönlichkeitsprofil einzelner Beschäftigter erstellt wird? Der Gesetzentwurf 2010 der Bundesregierung über den Beschäftigtendatenschutz verstand darunter ein „Gesamtbild der wesentlichen geistigen und charakterlichen Eigenschaften oder des Gesundheitszustands des Betroffenen“. Wie wird die Erstellung eines solchen „Gesamtbilds“ ggf. ausgeschlossen?

5. Das dreiseitige Papier „Workday and Sanofi. Creating One Vision from Many“ enthält eine Reihe von Stellen, die auf eine Benutzung von Cloud Computing schließen lassen. Werden durch Workday Cloud-Anwendungen benutzt? Wenn ja, sind die nötigen Vorkehrungen getroffen, damit die Grundsätze über die Auftragsdatenverarbeitung im Inland wie im Verhältnis zum Nicht-EU-Ausland eingehalten werden? Zu deren Inhalt s. näher Weichert DuD 2010, 679, 686

6. Aus dem Papier wird weiter deutlich, dass auch mit Hilfe mobiler Geräte auf die Workday-Daten zugegriffen werden kann. Dabei werden ggf. Server in den USA oder in anderen Drittstaaten eingeschaltet. Kann die Verschlüsselung sicher stellen, dass insoweit kein Zugriff durch Dritte erfolgen kann, die sich ggf. für die Forschungsinteressen oder die Karrierewünsche bestimmter Personen interessieren?