Greve, Silke

Research Report

Cloud Computing

Study der Hans-Böckler-Stiftung, No. 329

Provided in Cooperation with:
The Hans Böckler Foundation

Suggested Citation: Greve, Silke (2016) : Cloud Computing, Study der Hans-Böckler-Stiftung, No. 329, ISBN 978-3-86593-237-2, Hans-Böckler-Stiftung, Düsseldorf

Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

STUDY

Nr. 329 · Juni 2016

CLOUD COMPUTING

Reihe Praxiswissen Betriebsvereinbarungen

Silke Greve

MF MITBESTIMMUNGS-FÖRDERUNG

BETRIEBS-VEREINBARUNGEN

Die Reihe Praxiswissen Betriebsvereinbarungen wird herausgegeben von Dr. Manuela Maschke, Hans-Böckler-Stiftung.

Die Hans-Böckler-Stiftung ist das Mitbestimmungs-, Forschungs- und Studienförderungswerk des DGB. Sie ist in allen ihren Aufgabenfeldern der Mitbestimmung als Gestaltungsprinzip einer demokratischen Gesellschaft verpflichtet. Sie wirbt für diese Idee, unterstützt Mandatsträger in Mitbestimmungsfunktionen und tritt für erweiterte Mitbestimmungsrechte ein.

Hans Böckler Stiftung
Mitbestimmung · Forschung · Stipendien

STUDY

Nr. 329 · Juni 2016

CLOUD COMPUTING

Reihe Praxiswissen Betriebsvereinbarungen

Silke Greve

MF MITBESTIMMUNGS-FÖRDERUNG

BETRIEBS-VEREINBARUNGEN

Die Autorin

Dr. Silke Greve ist Juristin und Rechtsanwältin bei AfA Frankfurt mit dem Schwerpunkt Arbeits- und Datenschutzrecht.

Redaktion
Dr. Manuela Maschke

Kontakt
Telefon +49 211 7778-288
betriebsvereinbarung@boeckler.de

ISBN: 978-3-86593-237-2

Satz: DOPPELPUNKT, Stuttgart

INHALT

INDEX ICONS

→| Die Kennung am Ende des Zitats bezeichnet die Quelle und den Standort der Vereinbarung im Archiv. Sofern blau unterlegt, gelangen Sie direkt zur Vereinbarung in der Online-Datenbank.

ZUSAMMENFASSUNG

Die Sichtung des Archivs Betriebliche Vereinbarungen der Hans-Böckler-Stiftung ergab 13 Vereinbarungen aus 10 unterschiedlichen Branchen, die sich direkt oder indirekt mit dem Thema Cloud Computing beschäftigen und Gegenstand der vorliegenden Auswertung wurden. Angesichts der in den letzten Jahren stark ansteigenden Verwendung von cloudbasierten Anwendungen in Unternehmen ist dies eine verschwindend geringe Zahl, zumal sich mehrere Vereinbarungen auf die gleiche Software beziehen.

Die Materie weist jedoch neben der geringen Regelungsanzahl noch weitere Besonderheiten auf: Zum einen war aus den vorliegenden Vereinbarungen größtenteils nicht ersichtlich, dass es sich um Anwendungen handelt, die nicht mehr im Unternehmen selbst angesiedelt sind. Vielmehr konnte die Tatsache, dass eine Cloud-Datenverarbeitung im Hintergrund steht, oft nur aus den bekannten Namen der Software selbst geschlossen werden. Dabei ist gerade die cloudgestützte Datenverarbeitung selbst stark regelungsbedürftig. Zum einen ist oft nicht klar erkennbar, wo sich die Server-Standorte befinden und welchen Umfang der Zusammenschluss von Server-Farmen weltweit annehmen kann, wenn die Software in Auftragsspitzen die größtmögliche Auslastung erzielt. Datenschutzrechtlich kann jedoch nicht abgewichen werden von dem Grundsatz, dass gerade auch der Ort der Datenverarbeitung ein wesentliches Kriterium für die Sicherheit der Mitarbeiterdaten darstellt. Denn so sicher Regelungen in Deutschland sein können – wenn die Daten ins außereuropäische Ausland transportiert werden, entstehen gewaltige Regelungslücken, da dort geltende Gesetze oftmals keinen Schutz bieten.

Zum anderen wurden die bei der außereuropäischen Cloud-Datenverarbeitung zwingend notwendigen vertraglichen Regelungen zwischen Arbeitgeber und Software- bzw. Cloud-Anbieter selten in den betrieblichen Regelungen erwähnt. Ein Mitbestimmungsgremium kann seinen Schutzpflichten jedoch nur nachkommen, wenn der Arbeitgeber hier seine Auflagen erfüllt – nämlich die Absicherung der Datenströme durch Auftragsdatenverarbeitungsverträge oder den Abschluss der EU-Standardvertragsklauseln.

Diese und viele weitere Punkte sind oftmals jedoch noch weitestgehend ungeklärt. Die untersuchten Vereinbarungen stammen überwiegend aus den letzten drei Jahren und es wäre zu erwarten gewesen, dass sich mit dem Aufkommen der Verlagerungswellen von Kommunikationsdaten oder Reisekostenabrechnungsdaten in die internationalen Clouds die innerbetrieblichen

Regelungen verschärfen. Viel hat sich hier jedoch in den letzten Jahren nicht getan, so dass grundlegende Regelungspunkte unzureichend ausgestaltet sind oder teilweise ganz fehlen. Es scheint ein zunehmendes Problem zu sein, dass die Ausgestaltung der digitalen Informationsverarbeitung nicht mehr verstanden wird. Die Folge wird sein, dass ohne sachkundige Unterstützung kaum noch eine Vereinbarung rechtssicher abgeschlossen werden kann, um die Daten der Beschäftigten ausreichend zu schützen. Es wird hier noch viel Arbeit auf die Gremien zukommen.

VORWORT

Cloud Computing bedeutet, dass IT-Software, IT-Hardware sowie diverse Anwendungen von einem Drittanbieter über das Internet zur Verfügung gestellt und entstehende Daten entsprechend in einer Cloud gespeichert werden. Die bisher im lokalen Rechenzentrum vorgehaltenen IT-Ressourcen von Unternehmen sind das Geschäftsmodell und werden je nach Nutzung mit dem, der sie bereitstellt, abgerechnet. Unternehmensinterne Rechenzentren gehören der Vergangenheit an. Längerfristige Investitionen für Technologie werden reduziert, es entstehen vor allem noch operationale Kosten für den Dienstleister. Zur Verfügung gestellt wird alles was denkbar ist: IT-Infrastruktur, Netz-Plattformen, Speicherkapazitäten, Abwicklung von Geschäftsprozessen etc. Die Arbeit von IT-Abteilungen verändert sich, sofern sie überhaupt noch im Unternehmen existieren. Zahlreiche Arbeitsabläufe können ver- und ausgelagert werden, weil via Cloud der Arbeitsort nicht mehr das Unternehmen selbst sein muss.

Je nachdem wo Daten gespeichert werden, drängen sich verstärkt Fragen zum Datenschutz und zur Datensicherheit auf. Safe Harbour ist ein entsprechendes Stichwort. Dabei geht es darum, dass personenbezogene Daten aus EU-Staaten in externen Clouds in den USA gespeichert werden, obwohl das Datenschutzniveau der USA nicht dem europäischen Schutzniveau entspricht. Safe Harbour (sicherer Hafen) ist ein Verfahren und soll das Schutzniveau gewährleisten. Inzwischen wurde diese Regelung gekippt und soll durch ein neues „EU-US-Datenschutzschild“ ersetzt werden.

Wir haben für die Analyse 13 betriebliche Vereinbarungen der Jahre 2009 bis 2014 gesucht, ausgewählt und ausgewertet. Es wird gezeigt, welche Regelungstrends zur Gestaltung von Cloud Infrastrukturen inzwischen bestehen und wie betriebliche Akteure das Thema aufgreifen. Mit den Analysen verfolgen wir nicht das Ziel, Regelungen zu bewerten, die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen, Hinweise und Anregungen für die Gestaltung eigener Vereinbarungen zu geben.

Weitere Hinweise finden Sie im Internet unter
www.boeckler.de/betriebsvereinbarungen

Wir wünschen eine anregende Lektüre!

Dr. Manuela Maschke

1 RAHMENBEDINGUNGEN

1.1 Ansatzpunkte für die vorliegende Analyse

Die Meldungen in Presse- und Fachveröffentlichungen zu Cloud Computing variieren in den letzten Jahren stark. Berichte über Zugriffsmöglichkeiten von US-amerikanischen und europäischen Sicherheitsbehörden auf Datenwolken wechseln sich ab mit Ankündigungen über neuartige homomorphe Verschlüsselungstechnologien, die die Datenhaltung in Clouds sicherer machen sollen (vgl. Kirsch 2011 und Dr. Datenschutz 2013). Erst vor kurzer Zeit entschied ein amerikanischer Richter, dass er Zugriffe auf Daten, die in europäischen Clouds gespeichert sind, anordnen dürfe und wird so zum Schreckgespenst der IT-Industrie, die die Cloud-Daten vor dem Zugriff der NSA in Sicherheit bringen wollte (vgl. Schröder/Spieß 2014).

Bei all dem ist Cloud Computing trotzdem die Zukunft der Datenverarbeitung. Aufgrund der Flexibilität und allzeitigen Verfügbarkeit, die das Datenvorhalten in der Speicherwolke ermöglicht, wird es sinnvollerweise kein Zurück zu ortsgebundenen Lösungen geben. Genau dies ist der Anknüpfungspunkt, wenn es um die Frage der Regelung von unternehmensseitiger Datenspeicherung geht: Viele der heutigen Anwendungen greifen bereits auf Daten zu, die nicht mehr im Betrieb vorgehalten werden, sondern über Dienstleister kostengünstig aber extern bereitgestellt werden. Das Wissen jedoch, wo genau die betrieblichen Daten – beispielsweise Beschäftigtendaten – heute gespeichert sind, ist oft kaum oder gar nicht vorhanden.

Betriebliche Interessenvertretungen greifen dabei auf Regelungen zurück, die noch aus Zeiten stammen, als die Daten vor Ort blieben und damit höchstens dem Risiko betrieblicher Geheimnisverletzungen ausgesetzt waren. Solche Gefahren waren jedoch wesentlich besser in den Griff zu bekommen. Die handelnden Akteure waren bekannt, die rechtliche und tatsächliche Kontrolle konnte relativ einfach ausgeübt werden. Allenfalls gegenläufige Interessenlagen zwischen Arbeitgeber und Arbeitnehmern mussten beachtet und ausgeglichen werden. Heute kommen vollkommen neue Akteure hinzu: zum Beispiel Anbieter von cloudgestützten Lösungen, die ihren Sitz oft im Ausland haben. Sie richten ihr Hauptaugenmerk regelmäßig nicht auf (deutsche) Datenschutzgesetze, sondern auf eine mögliche Effizienzsteigerung ihrer Produkte. Unternehmen werben mit Slogans wie „Cloud Your

Car – Fahrerüberwachung ist besser als Rätselraten“[1]. Anlässlich solcher Drittinteressen müssen Softwarelösungen auch vor dem Hintergrund notwendiger Auftragsdatenverarbeitungsverträge neu überdacht oder zumindest neu betrieblich geregelt werden.

Auf der Basis der bereits bestehenden Regelungen wird im Folgenden herausgearbeitet, ob Unternehmen und betriebliche Interessenvertretungen bereits einen Standard für den Umgang mit der Tatsache etabliert haben, dass sie die alleinige Kontrolle über die Daten aus der Hand geben. Es wird auch aufgezeigt, wie und wo versteckte Cloud-Lösungen hinter vermeintlich „einfachen“ Anwendungen stehen und welche betrieblichen Regelwerke daher Lücken in der Durchsetzbarkeit beinhalten – und wie diese geschlossen werden können.

Ein derart umfassendes Thema wie Cloud Computing lässt sich nicht vollständig für alle Einsatz- und Regelungsmöglichkeiten beschreiben. Ziel ist daher, die bestehenden Vereinbarungen und Richtlinien so aufzubereiten, dass den Nutzern unterschiedliche Vorgehensweisen differenziert ersichtlich werden. Hieraus können die betrieblichen Interessenvertretungen Handlungsstrategien ableiten, wenn sie im eigenen Unternehmen mit der Anforderung konfrontiert sind, neue Regelungen erstellen zu müssen.

1.2 Entwicklung des Cloud Computing

Mitte der 2000er Jahre sahen sich große Internet-Dienstleister mit dem Problem konfrontiert, ihre Anwendungen zu bestimmten Stoßzeiten nicht mehr in ausreichendem Leistungsumfang bereitstellen zu können. Um diesem Problem zu begegnen, entschied man sich, die (serviceorientierte) Architektur und die Dienste, die man zum Bewältigen der zum Teil stark schwankenden oder auch sehr hohen Nutzerzahlen entworfen und etabliert hatte, zu einem Produkt zu machen, das man nach außen hin anbietet: Das heißt, dass dieses Problem in Spitzenlastzeiten auf die Nutzer der Cloud zu verteilt wird[2]. Seitdem stehen Daten für vielfältigste Nutzergruppen zu allen Zeiten und an allen Orten zur Verfügung.

1 „Cloud Your Car – Fahrerüberwachung ist besser als Rätselraten“ (aktiv bis Juli 2015 unter https://cloudyourcar.com), heute: „Cloud Your Car – Start monitoring your drivers an stop guessing“, https://www.linkedin.com/company/cloud-your-car [22.2.2016].

2 Vgl. die Geschichte des Cloud Computing unter http://de.wikipedia.org/wiki/Cloud_Computing [22.2.2016].

Diese Entwicklung wirkte sich auch auf die Arbeitswelt aus. Im Zuge dessen, dass sich die Verfügbarkeit der Programme und Daten erhöhte und die Unternehmen gegebenenfalls Kosten reduzieren konnten, weil sie weniger oder gar keine Speichermedien mehr vorhalten mussten, wurden Fragen laut: Wie war etwa in arbeitsrechtlicher und sozialpolitischer Hinsicht mit der allzeitigen Verfügbarkeit umzugehen? Zusätzlich sahen sich betriebliche Interessenvertretungen und Unternehmen mit neuen Fragen der Datensicherheit und des Datenschutzes konfrontiert.

Diese Fragen sind bei Weitem nicht gelöst, sondern stehen in vielen Bereichen weiterhin ungeklärt im Raum. Angesichts des zusätzlichen Aufwands bei der faktischen und rechtlichen Regelung vieler Fragen bleibt abzuwarten, ob die Kostenersparnis sich langfristig bewahrheitet. Diverse Fragen müssen gelöst werden: zur Arbeitszeit (Arbeitszeitgesetz), zum Datentransfer in Drittländer ohne angemessenes Datenschutzniveau (Bundesdatenschutzgesetz) oder zur Durchsetzbarkeit von Haftungsansprüchen bei Ausfall der Systeme und hierdurch entstehenden finanziellen Schäden aufgrund von Arbeitsstillstand (internationales Privatrecht). Sie müssen zudem so gelöst werden, dass Arbeitnehmerrechte nicht verletzt werden und Beschäftigte nicht in für sie unverständlichen Zusammenhängen arbeiten müssen. Überlastung, diffuse Ängste, die innere Kündigung, Abkoppelung von Unternehmensinteressen – all das können Folgen sein, wenn Arbeitnehmer nicht mehr grundlegend darüber informiert sind, wie das, was sie tun, funktioniert oder wenn sie mit beständig steigenden Serviceproblemen konfrontiert werden.

In diesem Zusammenhang ist es oft schon für die Unternehmen selbst schwer, zu begreifen und darzustellen, wie die vielen Neuerungen „in der IT" funktionieren. Dies macht sie zu schlechten Ansprechpartnern für betriebliche Interessenvertretungen, die den Schutz der Mitarbeiter durchsetzen wollen und müssen. Die Folge dieser Intransparenz ist ein oft nicht mehr überschaubares Risiko, unternehmensseitig in Anhängigkeiten und – schlimmstenfalls – Handlungsunfähigkeiten hineinzugeraten. Hier müssen die Betriebs- und Personalräte oftmals Pionierarbeit leisten, wenn sie herausfinden wollen, wie sie die dynamischen Veränderungen in den Griff bekommen wollen. Aus den hier begutachteten und aufbereiteten Vereinbarungen und Richtlinien sollen sie Möglichkeiten ableiten können, wie sie auch die gesellschaftspolitischen Auswirkungen der wachsenden Entkoppelung der Datenverarbeitung in vernünftigere Bahnen lenken können.

Selbst wenn man in absehbarer Zeit die Erkenntnis gewinnt, dass die Kostenreduktion, die dem Datenspeicher Cloud zugeschrieben wurde und

wird, sich als marginal oder nicht vorhanden herausstellt, wird das Cloud Computing weiterhin die Zukunft der Datenverarbeitung sein. Alleine die erhöhte Verfügbarkeit der Daten, die Ressourcenreduzierung hinsichtlich der Speichermedien (und -materialien), die vielfältigeren Weiterentwicklungs- und Problemlösungsszenarien durch omniverfügbare und -kombinierbare Entwicklerteams mit allzeitigem Zugriff auf cloudbasierte Anwendungen werden die Entwicklung weg von ortsgebundenen Datenverarbeitungen forcieren.

Bezüglich der innerbetrieblichen Regelung dieser Art der Datenverarbeitung wird sich kurz- bis mittelfristig nicht mehr die Frage stellen, *wie* dieser Teil der Datenverarbeitung zu regeln ist. Vielmehr werden die jetzt angestoßenen Lösungsmöglichkeiten perspektivisch die Grundlage für jedwede Datenverarbeitung in Unternehmen – weil jedwede Beschäftigten- und Kundendatenverarbeitung über kurz oder lang in den Datenwolken dieser Welt stattfinden wird.

1.3 Stand der Vereinbarungen

Trotz der steigenden Anzahl der durch Cloud Computing zur Verfügung gestellten Anwendungen und Programme ist die Regelungslandschaft der Betriebsvereinbarungen ein scheinbar schlecht bestelltes Terrain. Zumindest finden sich wenige abgeschlossenen Vereinbarungen. Das mag daran liegen, dass die Vereinbarungen und Handlungsanweisungen sich zwar beispielsweise auf eine Software oder Ähnliches beziehen, die über die Cloud zur Verfügung gestellt wird, sich aber nicht direkt mit dem Cloud Computing auseinandersetzen oder dies betiteln. Alleine aus diesen Gründen ist es derzeit noch schwierig, die Thematik ganz zu erfassen und gar zu regeln. Gleiches gilt im Übrigen für die Bezeichnungen und weitere Standardisierungen innerhalb des Themenfeldes: Wenn schon keine zwingenden Standards gelten[3], wie und woran sollen sich Betriebs- und Personalräte dann für künftige Regelungen orientieren?

3 In der Broschüre des Bundesministeriums für Wirtschaft und Technologie „Das Normungs- und Standardisierungsumfeld von Cloud Computing“ (2012) werden alleine „die 19 wichtigsten“ deutschen, europäischen und internationalen Standardisierungsorganisationen aufgeführt, vgl. http://www.bmwi.de/DE/Mediathek/publikationen,did=476730.html [21.2.2016].

Nur wenige große Projekte beschäftigen sich beispielsweise mit dem gesamten Komplex der „Industrie 4.0, Smart factory“[4] und beziehen dabei selbstverständlich auch das Cloud Computing ein. Daneben stehen vielfach kleinere, oftmals in Einzelberatungen entwickelte Falllösungen (vgl. Ruchhöft 2012 und Heidemann 2012), die bisher jedoch einen geringeren Verbreitungsgrad besitzen. Zur Verfügung stehen dagegen zahlreiche rechtliche und technische Auseinandersetzungen mit umfangreichen Beschreibungen des gesamten Themenfeldes, die jedoch für die praktische Anwendung für die Betriebs- und Personalräte selten sinnvoll sind (vgl. Lehmann/Giedke 2013 und BSI 2012). Wesentlich für die praktische Arbeit ist es, einen Überblick über vorhandene Regelungen zu bekommen, deren Verwendbarkeit in der Praxis möglichst bereits schon getestet wurde und deren Modularität die einzelnen Regelungsinhalte anpassungsfähig macht. Nur so kann der mit einer neuen Anwendung konfrontierte Betriebs- oder Personalrat schnell und möglichst rechtssicher Regelungen entwickeln.

Denn dies wird zunehmend dringlicher. Nach einer Pressemitteilung des Statistischen Bundesamtes vom 19. Dezember 2014[5] setzen 12 % der Unternehmen auf Cloud Computing. Dabei nutzen bereits 27 % der Unternehmen mit mehr als 250 Beschäftigten, aber nur 10 % der Unternehmen mit 10 bis 49 Beschäftigten cloudgestützte Datenverarbeitungen. Die Gründe hingegen, warum manche Betriebe von Cloudlösungen absehen, werden mit Sicherheitsbedenken (37 %) und rechtlichen Unsicherheiten (32 %) angegeben. Am häufigsten werden die Datenwolken für die Speicherung von Daten (56 %), für E-Mails (46 %) und als Basis für den Betrieb von Datenbanken (34 %) verwendet. Allerdings wollen sich viele Unternehmer auch nicht vollständig von den externen Anbietern abhängig machen. Die Gründe, warum manche Firmen nur eingeschränkt auf cloudbasierte Anwendungen zurückgreifen, sind die Angst vor Sicherheitsrisiken (47 %), wiederum die Unsicherheit in rechtlicher Hinsicht (37 %) und – datenschutzrechtlich sehr relevant – die ungeklärten Fragen bezüglich der geografischen Server-Standorte (36 %).

Eine Studie der Bitkom (2014) in Zusammenarbeit mit der Wirtschaftsprüfungs- und Beratungsgesellschaft KPMG zeigt zwar andere absolute Prozentwerte. Insgesamt ist aber auch hier klar erkennbar: Die Größe des Unter-

4 Vgl. Praxisblätter für Betriebsräte und Aufsichtsräte der Hans-Böckler-Stiftung zum Thema „Produktionsarbeit im Wandel – Industrie 4.0, Smart factory“ unter www.boeckler.de/46972.htm#cont_46981 [21.2.2016].

5 Vgl. Statistisches Bundesamt 2014, https://www.destatis.de/DE/PresseService/Presse/Pressemitteilungen/2014/12/PD14_467_52911pdf.pdf?__blob=publicationFile [21.2.2016].

nehmens spielt eine entscheidende Rolle bei der Frage, ob Cloud-Lösungen genutzt werden oder nicht. Je größer ein Unternehmen ist, desto größer ist auch die Bereitschaft, auf diese Art der ausgelagerten Datenverarbeitung zurückzugreifen. Interessant ist hieran, wie nach dem NSA-Skandal die Unternehmen gerade in Bezug auf das Cloud Computing reagierten: 31 % erhöhten die Sicherheitsanforderungen, 13 % stellten geplante Cloud-Projekte zurück und 11 % gaben sogar an, bereits bestehende Cloud-Lösungen wieder aufgegeben zu haben (ebd.).

Das Statistik-Portal Statista kommt zwar auf andere absolute Prozentzahlen, zeigt aber ebenfalls: Die Bereitschaft, cloudgestützte Anwendungen im Unternehmen einzuführen, ist seit dem Jahr 2011 kontinuierlich gestiegen und die Großunternehmen sind hierbei Vorreiter.[6] Nicht erstaunlich ist es, dass gerade die Informations- und Kommunikationsbranche mit 45 % führend ist bei der Nutzung von Cloud-Computing-Lösungen im Unternehmen. Es folgen freiberufliche, wissenschaftliche und technische Dienstleistungen mit 27 %. Schlusslicht ist hier das Baugewerbe mit 14 %.

Der Cloud-Monitor 2015 der Bitkom[7] zeigt zudem, dass 39 % der befragten Unternehmen auf Private Clouds setzen, wohingegen nur 16 % die Public Cloud bevorzugen.

1.4 Neueste Entwicklungen

Das Urteil des Europäischen Gerichtshofes (EuGH) zur Safe-Harbor-Zertifizierung[8] hat in Europa für große Aufregung gesorgt. Zwar war zunächst nur diese eine Zertifizierung für den transatlantischen Datenverkehr plötzlich obsolet geworden; dennoch wurden schnell Meinungen laut, wonach vom „Safe-Harbor-Urteil“ auch alle anderen Legitimationen zum Datenaustausch mit Staaten ohne angemessenes Datenschutzniveau umfasst sein könnten,

6 Vgl. Nutzung von Cloud Computing in Unternehmen in Deutschland in den Jahren 2011 bis 2014 (http://de.statista.com/statistik/daten/studie/177484/umfrage/einsatz-von-cloud-computing-in-deutschen-unternehmen-2011/ [22.2.2016]) und im Jahr 2014 nach Unternehmensgröße (http://de.statista.com/statistik/daten/studie/305563/umfrage/einsatz-von-cloud-computing-in-deutschen-unternehmen-nach-groesse/ [22.2.2016]).

7 Vgl. Bitkom Research GmbH (2015) https://www.bitkom.org/Publikationen/2015/Studien/Cloud-Monitor-2015/Cloud_Monitor_2015_KPMG_Bitkom_Research.pdf [21.2.2016].

8 Vgl. EuGH, Urteil vom 6.10.2015, C-362/14, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 [22.2.2016].

wie beispielsweise die EU-Standardvertragsklauseln oder Corporate Binding Rules. „Der EuGH hat ein Monster geschaffen“ titelte die Zeit online in diesem Zusammenhang (vgl. Beuth 2015).

Dies wäre für die gesamte Cloud-Industrie tatsächlich ein erhebliches Problem. Gerade bei der Unternehmensdatenverarbeitung spielen personenbezogene Daten eine entscheidende Rolle. Und da die Cloud-Datenverarbeitung in nur sehr geringem Umfang in Europa stattfindet, wäre hiervon der größte Teil der Unternehmensdatenflüsse betroffen.

Was sagt das Urteil genau aus? Safe Harbor ist mit sofortiger Wirkung gestoppt – der Datenverkehr auf der Basis dieses Abkommens ist ab sofort nicht mehr legitimiert. Die EU-Kommission hatte im Jahr 2000 Safe Harbor als Legitimation für internationalen Datentransfer anerkannt. Der EuGH erklärt diese Anerkennung nun für ungültig, weil sie eine pauschale Öffnungsklausel enthält, nach der US-Behörden (unter bestimmten Voraussetzungen) auf Daten von EU-Bürgern zugreifen können. Die Entscheidung des EuGH bezieht sich zwar zunächst ausdrücklich nur auf Safe Harbor. Die Formulierungen im Urteil sind jedoch so gewählt, dass man sie ebenfalls auf die EU-Standardvertragsklauseln oder Binding Corporate Rules anwenden könnte: „Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens.“ Dies könnte auch bedeuten: Alles, was den US-Behörden den Zugriff auf EU-Nutzerdaten gestattet, verstößt gegen den Wesensgehalt der EU-Grundrechtecharta. Und dies gilt, vereinfacht gesagt, auch für die EU-Standardvertragsklauseln. Denn US-Gesetze wie der Patriot Act, die solche Datenzugriffe gestatten, werden auch von den EU-Standardvertragsklauseln nicht eingeschränkt.

Ob die nationalen Datenschutzbehörden dies künftig genauso einschätzen, bleibt zunächst abzuwarten. Aktuell ist zwar ein Datenaustausch auf der Basis von Safe Harbor nicht mehr möglich; die EU-Standardvertragsklauseln sollten jedoch so lange beibehalten werden, bis sich die Behörden eindeutig dazu geäußert haben. Denn Fakt ist: Gerade in Bezug auf das Cloud Computing wird es eine Lösung geben müssen.

Weitere Informationen hierzu sowie zu anderen aktuellen Entwicklungen und offenen Fragen finden sich in Kapitel 4.

2 REGELUNGSINHALTE UND VEREINBARUNGEN

Wer mehr wissen möchte
Auszüge aus Vereinbarungen und Recherchemöglichkeiten zu diesem Thema finden sie hier:
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166

Das Thema Cloud Computing wird zum jetzigen Zeitpunkt sehr unterschiedlich in den vorliegenden Vereinbarungen behandelt. Es fällt vor allem auf, dass Regelungen fehlen, die sich tatsächlich auf die dahinterstehende Struktur einer cloudgestützten Datenverarbeitung beziehen. Die Frage nach dem verwendeten Cloud-Modell wird nicht beantwortet: Ob die Form des Software as a Service (SaaS), Platform as a Service (PaaS) oder Infrastucture as a Service (IaaS) gewählt wurde, ist aus dem Untersuchungsmaterial nicht ersichtlich. Ebenso wenig kann abgeleitet werden, ob es sich um eine Public Cloud, eine Private Cloud oder ein Hybrid Cloud handelt.

Größtenteils wird durchaus eine cloudgestützte Software zum Regelungsgegenstand der Vereinbarungen gemacht (vgl. Kap. 2.2), allerdings ohne dies direkt zu benennen. Vereinzelt wird nur sehr allgemein darauf verwiesen, wie mit dem Thema Cloud Computing im Unternehmen umgegangen werden sollte (Kap. 2.1).

2.1 Allgemeine Hinweise auf die Datenverarbeitung in der Cloud

Wer mehr wissen möchte
Auszüge aus Vereinbarungen zu diesem Thema finden sie hier: http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

In Vereinbarungen, die das Thema Cloud Computing eher marginal behandeln wie z. B. der nachstehend zitierten Dienstvereinbarung zur Nutzung von Informationstechnologie, wird durchaus anerkannt, dass sich die cloud-

basierte Datenverarbeitung in ihrem Wesensgehalt von der bisher eher lokalen Datenverarbeitung unterscheidet. Dieses Risiko wird beispielsweise implizit angesprochen, indem erhebliche Hürden für die Cloud-Nutzung geschaffen werden. Ein grundsätzliches Verbot der Nutzung von Cloud-Anwendungen, das nur unter erheblichem Aufwand gelockert oder aufgehoben werden kann, spricht für das Bewusstsein der handelnden Akteure, es hier mit einer schwer zu kontrollierenden Art der Datenverarbeitung zu tun zu haben.

> „Nutzung von Cloud-Computing (Speicherung von Daten an unbekannten Lokationen im Internet)
> Die Nutzung von Cloud-Computing ist grundsätzlich nicht gestattet. Zur ausnahmsweise dienstlichen Nutzung von Cloud-Computing muss die schriftliche Bestätigung des dienstlichen Interesses durch die/den Geschäftsbereichsleiterin bzw. ReferatsleiterIn […] unter Beteiligung der Stabsstelle für Datenschutz und IT-Sicherheit […] und des Gesamtpersonalrates vorgelegt und besonders begründet werden. […] entscheidet dann gemeinsam mit dem zuständigen Fachvorstand und dem IT-Vorstand über die beantragte Nutzung von Cloud-Computing."
> →I Öffentliche Verwaltung, 090201/523/2012

Teilweise wird ohne jegliche Begründung die Nutzung bestimmter, namentlich genannter Dienste untersagt. Es handelt sich hierbei um cloudgestützte Datenverarbeitung (Dropbox, iCloud), ohne dass dies explizit angesprochen wird.

> „Geräte-Backup
> Backup und Synchronisation des Gerätes dürfen nur auf zugelassenen Firmencomputern und nicht auf privaten PCs durchgeführt werden. Firmendaten dürfen nicht auf entfernten Servern, wie Dropbox oder iCloud, gespeichert werden."
> →I Chemische Industrie, 090202/190/2012

Tatsächlich kann sich die cloudgestützte Datenverarbeitung hinter fast jeder Thematik „verstecken", weshalb in jedem Unternehmen die in den letzten Jahren abgeschlossenen Vereinbarungen einer genaueren Überprüfung dahingehend bedürften. Im Folgenden wird beispielsweise die Durchführung einer Beschäftigtenbefragung geregelt. Aus dem Text und dem Fragenkatalog dieser Vereinbarung wird zwar anhand der Software-Bezeichnungen (Share-

point, Lync) erkennbar, dass heute möglicherweise Cloud-Lösungen im Unternehmen genutzt werden – deutlich beschrieben wird dies jedoch nicht.

> „Die Befragung erfolgt online per SharePoint, dadurch wird die Anonymität gewährleistet. Die Fragen sind Bestandteil dieser Vereinbarung (s. Anlage 1).
> ‚[…] Die zukünftige Durchführung regelmäßiger Konferenzen z. B. via Lync mit anderen Ideenkoordinatoren fände ich […]'."
> ➔ Maschinenbau, 110400/24/2012

Das Problem hierbei: Die Vereinbarung stammt aus dem Jahr 2012. Die nun im Jahr 2012 noch nicht cloudbasierten Anwendungen von Microsoft werden heute längst cloudgestützt angeboten. Die vorliegende Vereinbarung ist jedoch weiterhin gültig. Es besteht also die Möglichkeit, dass sich diese Vereinbarung heute auf derlei Cloud-Lösungen bezieht. Ob dem so ist oder nicht, ist zumindest anhand der vorliegenden Vereinbarung nicht ersichtlich, da genauere Bezeichnungen wie etwa „Lync Server" oder „Lync online".

2.2 Regelungspunkte bei cloudbasierter Datenverarbeitung

Wer mehr wissen möchte
Auszüge aus Vereinbarungen zu diesem Thema finden sie hier: http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

2.2.1 Regelungsgegenstand

Anders als bei anderen Regelungsmaterien stellt die Formulierung des Gegenstands in Vereinbarungen zu cloudbasierter Software oftmals ein größeres Problem dar. Generell wird in betrieblichen Regelungen unter diesem Punkt umrissen, was der Grund zum Abschluss der Vereinbarung ist. Bei IT-Betriebsvereinbarungen wird hier die Software möglichst genau bezeichnet und ihr Wirkungsumfang kurz dargestellt. Es sollten daher die genaue Versionsnummer genannt und die eingesetzten Module oder Tools der Anwendung

aufgelistet werden. Eine genauere Beschreibung folgt dann zumeist an einer späteren Stelle des Vereinbarungstextes.

Bei cloudbasierter Software könnte man nun annehmen, dass die Beteiligten zum einen die Software als solche beschreiben und zum anderen zumindest das Modell der Cloud und deren genaue Bezeichnung aufführen. An späterer Stelle der Regelungen könnte dann vertieft auf die Datenströme in und aus der Cloud eingegangen werden. Dies ist jedoch erstaunlicherweise in keiner der vorliegenden Vereinbarungen der Fall. Dass es sich bei diesen Vereinbarungen um solche handelt, die einen cloudbasierten Softwareeinsatz regeln, kann ausschließlich aus den Namen der Anwendungen geschlossen werden; und dies auch nur dann, wenn hierzu Hintergrundinformationen aus anderen Quellen hinzugezogen werden.

Beispielsweise ist beim Einsatz des Reisekostenabrechnungstools Concur alleine aus dem Namen und weiteren, zusätzlich recherchierten Hintergrundinformationen zu erkennen, dass es sich hierbei um eine Software der Firma Concur Technologies Inc. handelt, die diese Abrechnungssysteme webbasiert anbietet. In einer Vereinbarung von 2009 wird hierauf mit keinem Wort Bezug genommen. Das Reisekostenmanagementsystem ist demnach vor und nach der Übernahme eine SaaS-Cloud-basierte Software, was jedoch in der Formulierung des Vereinbarungsgegenstandes keine Erwähnung findet.

> „Die Betriebsvereinbarung regelt die Anwendung der elektronischen Spesen- und Promotionabrechnung Concur bei der [Firma]; einschließlich der Verwendung und Auswertung mitarbeiterbezogener Daten.
> Die Betriebsvereinbarung gilt für alle technischen und organisatorischen Maßnahmen, die mit der Einführung, Anwendung und Erweiterung von Concur verbunden sind, unabhängig davon, ob diese Maßnahmen betriebsintern oder durch Dritte durchgeführt werden. Sie gilt auch für Testläufe, falls dabei Mitarbeiterdaten erhoben, verarbeitet oder genutzt werden.
> Concur wird ausschließlich zu buchhalterischen Zwecken einer elektronischen Spesen- und Promotionabrechnung eingesetzt. Concur ist in Anlage 1 zu dieser Betriebsvereinbarung näher beschrieben.
> IT-System: Concur Travel & Expense, Version 7.1 (Intranet-Anwendung) (nachfolgend: Concur)."
> →| Großhandel (ohne Kfz.), 090503/43/2009

In einer weiteren Vereinbarung aus dem Jahr 2014, als SAP bereits die Übernahme des Anbieters Concur Technologies, Inc. abschließend betrieb, um sein Cloud-Geschäft umfassend zu erweitern, wird ebenfalls der Gegenstand der Vereinbarung nur mit dem allgemeinen Begriff Concur bezeichnet, ohne eine Versionsnummer zu benennen oder die Art der Cloud näher zu beschreiben. Immerhin wird etwas ausführlicher darauf eingegangen, dass das System mit externen Anbietern verbunden ist. Aber dies könnte auch lediglich auf ein Outsourcing hindeuten. Die Risiken, die eine cloudgestützte Verarbeitung mit sich bringt, sind auch hier nicht erkennbar.

> „[Die Firma] führt deutschlandweit an all seinen Standorten das neue Kostenabrechnungssystem Concur ein, das alle gegenwärtig für die Erfassung und Bearbeitung von Kostenforderungen genutzten Systeme ersetzen wird.
> Concur ist ein integriertes System, das mit der Kreditorenbuchhaltung (Accounts Payable System) für die Zahlung von Mitarbeiter-Reisekosten und dem Corporate Credit Card Anbieter verbunden ist. Es wird zur Verfügung gestellt von der [Firma], die insoweit als Auftragsdatenverarbeiter für [die Firma] tätig wird."
> ➔ Börse/Makler, 090203/76/2014

Eine weitere als cloudbasierte Anwendung bekannte Software für das Kundenbeziehungsmanagement (Salesforce) wird in der folgenden Vereinbarung benannt. Zudem erfolgt eine Erklärung zum Einsatz im Unternehmen – dass es sich um eine SaaS- oder PaaS-Cloud-Lösung handelt, ist jedoch an keiner Stelle erkennbar. Dies ist gerade vor dem Hintergrund problematisch, dass hierbei erhebliche Informationen über die Beschäftigten gesammelt werden können, die das System bedienen. Insbesondere kann das Kommunikationsverhalten der Arbeitnehmer mit den Kunden analysiert werden, da Verknüpfungen mit weiteren Social-Media-Anwendungen möglich sind.

> „Das elektronische Vertriebs- und Kunden-Instrument (englisch: CRM Customer Relationship Management Tool) Salesforce.com hat zum Ziel, die Zusammenarbeit mit unseren Kunden zu verbessern und effizienter zu gestalten. […] Dem Unternehmen dient es zu einer verbesserten internen Kommunikation sowie zur schnelleren Kommunikation mit dem Kunden als auch zur besseren Quali-

> fizierung von potenziellen Neukunden. […] Für die Mitarbeiter soll es teamorientiertes Arbeiten mit vernetzten Informationen fördern."
>
> →I Mess-, Steuer- und Regelungstechnik, 090203/60/2013

Eine weitere Vereinbarung mit dem gleichen Regelungsgegenstand benennt ebenfalls das System, ohne die dahinterstehende Cloud zu erwähnen. Beim Regelungsgegenstand wird hier ebenfalls Wert auf die Gründe des Einsatzes im Unternehmen gelegt. Die qualitativ andersartige Datenverarbeitung in einer dynamischen, externen Umgebung wird jedoch nicht thematisiert.

> „Die Implementierung von Salesforce CRM ist Teil eines langfristigen Plans, nur noch aus einer einzigen Quelle Daten über Geschäftsbeziehungen zu ziehen und zur Betrachtung einer Kundenbeziehung heranzuziehen. Dadurch sollen insbesondere die Prozesse und Aktivitäten rund um den Kunden transparenter werden."
>
> →I Börse/Makler, 090203/77/2014

Ähnliches gilt für den Einsatz von Tools aus dem Unternehmen ServiceNow, das sich selbst als „The Enterprise Cloud Company" bezeichnet. Obwohl das Unternehmen ausschließlich Cloud-Lösungen anbietet, was durch eine kurze Recherche leicht erkennbar wäre, informiert die Vereinbarung nicht über die Tatsache, dass die Beschäftigtendaten in einer Cloud verarbeitet werden.

> „Gegenstand dieser Anlage ist die Einführung und Nutzung des ASSM (After Sales Service Management) und eQMS Tools von ServiceNow in der [Firma] als Nachfolgesoftware des bisherigen Tools PowerHelp ab 25.11.2013."
>
> →I Anonym, 090203/71/2013

Dagegen wäre eine konkrete Benennung der Cloud-Datenverarbeitung bereits im Regelungsgegenstand gerade deswegen so sinnvoll, weil dies jeden folgenden Regelungspunkt beeinflussen würde. Es wäre dann von Beginn an klar: Die Beteiligten müssen bewusst und detailliert eingehen auf Fragen des bzw. der Speicherorte(s), der externen Zugriffsberechtigten und auch der Länder, in denen die Arbeitnehmerdaten verarbeitet werden.

2.2.2 Zweckbestimmung

Bei Vereinbarungen, die eine Softwareverwendung regeln, ist die genaue Bestimmung des Einsatzzwecks der IT-Ressource entscheidend für jede weitere Frage der Datenerhebung, -verarbeitung oder -löschung. Ausschließlich anhand der Zweckbestimmung kann sich entscheiden, welche personenbezogenen Daten der Beschäftigten für die Nutzung der Anwendung zwingend notwendig sind. Sogar die Frage, ob die Beschäftigtendaten überhaupt per Arbeitgeberanweisung erhoben werden dürfen oder ob es den Beschäftigten freistehen muss, die Software zu nutzen und damit ihre Daten freiwillig zur Verfügung zu stellen, hängt von der Zweckbestimmung ab. Denn gemäß § 32 BDSG dürfen nur „erforderliche" Beschäftigtendaten verwendet werden und auch nur insoweit es dem Beginn, der Durchführung oder der Beendigung des Arbeitsverhältnisses dient. Stützt sich der Einsatz der Software also auf ein berechtigtes Unternehmensinteresse, ist die Datenverarbeitung erforderlich, jedoch nur in dem Umfang, in dem es nach Art, Qualität und Dauer notwendig ist. Dies gilt umso mehr für den Einsatz cloudbasierter Software. Da hierbei der Kreis der Beteiligten (Arbeitgeber, Cloud-Dienstleister, Servereigentümer etc.) größer ist als bei unternehmensinternen IT-Lösungen, müssen beispielsweise die Zugriffsberechtigungen intensiver durchleuchtet und geregelt werden.

Als Beispiel kann hier wieder das Reisekostenmanagement der Unternehmen dienen. Dass es sich hierbei um eine für die Durchführung von Beschäftigungsverhältnissen erforderliche Aufgabe handelt ist unbestritten. Ob diese Aufgabe notwendigerweise unter Zuhilfenahme einer cloudbasierten Software bewältigt werden muss, wäre jedoch schon eine Einzelfallprüfung, die selten positiv beantwortet werden kann (vgl. ablehnend Wedde 2014, S. 17). Möglicherweise lässt sich dies in internationalen Großunternehmen begründen, da diese mit tausenden von Buchungsvorgängen konfrontiert sind. Ob aber bei einem kleinen mittelständischen Unternehmen die Effizienzsteigerung und Kostenreduktion durch eine Cloud-Nutzung derart ins Gewicht fiele, um die Weitergabe der Arbeitnehmerdaten in unsichere Speicherorte zu rechtfertigen, muss dringend hinterfragt werden. Es sei darauf hingewiesen, dass als Grund für einen Softwareeinsatz bzw. einen cloudbasierten Softwareeinsatz wirtschaftliche Erwägungen alleine nicht ausreichen. Hierzu müssten nähere Angaben gemacht werden, um die Barriere der Erforderlichkeit zu durchbrechen. Die Ausführungen in der nachstehenden Vereinbarung genügen demnach nicht zur Begründung der Nutzung eines cloudbasierten Reisekostenmanagement-Tools, wenngleich der Zweck als solcher

(Erhebung der Mitarbeiterdaten für das Reisekostenmanagement) durchaus die Erforderlichkeitskriterien erfüllt.

> Zweck von Concur
> Concur ersetzt alle bisherigen Systeme zur Eingabe und Bearbeitung von Reisekosten. Da es internetbasiert ist, ist sowohl die Antragstellung auf Reisekostenerstattung sowie die Freigabe jederzeit und ortsunabhängig möglich. Die mit der Corporate Credit Card getätigten Umsätze werden automatisch mit dem Concur System verknüpft und können dem Reisekostenantrag des Mitarbeiters zugeordnet werden.
> Concur wird Kreditkarten-Transaktionsdaten direkt vom Corporate Kreditkarten-Anbieter einpflegen und hat eine direkte Schnittstelle zum Kreditoren-System. Dadurch wird die Abwicklung von Reisekosten, insbesondere der Antragstellungs- und Prüfungs- und Genehmigungsprozess erheblich vereinfacht und die Zahlungen an Einzelpersonen und an den Corporate Credit Card Anbieter beschleunigt."
> ➔ Börse/Makler, 090203/76/2014

Gerade deswegen ist es wichtig, dass bei der Zweckbestimmung des Softwareeinsatzes, die der Zweckbestimmung der zu erhebenden Beschäftigtendaten vorausgeht, detailliert auf die verwendete Cloud-Lösung eingegangen wird. Wird es beispielsweise möglich, zusätzliche Funktionen zu nutzen, die nur in einer cloudbasierten Anwendung zur Verfügung stehen, kann sich dies auf die Rechtfertigung der Erforderlichkeit der Datenverarbeitung in der Cloud eventuell positiv auswirken. Einen solchen – zusätzlichen – Zweck genau zu beschreiben, ist unter anderem deswegen notwendig, weil sich hieran auch die Dauer der Datenspeicherung messen lassen muss. Genügt für den exakt benannten Zweck nämlich z. B. nur eine anonymisierte Speicherung, ist diese zu bevorzugen. Eine pauschale oder stichpunktartige Benennung der Zwecke alleine ist jedoch nie ausreichend.

> „Zweck von Salesforce CRM
> Das Customer Relationship Management Tool (CRM) ist ein Modell, um als Unternehmen Nutzen aus der Interaktion mit Kunden, Maklern und zukünftigen Absatzchancen zu ziehen. Salesforce ist somit ein Werkzeug, um CRM-Geschäftsprozesse organisieren, zu

automatisieren und zu synchronisieren. Die Nutzung von Chatter als Teil von Salesforce CRM erfolgt auf freiwilliger Basis.
[…]
Zweck der Datenerhebung, -verarbeitung oder -nutzung
☒ Korrespondenz
☒ Antragsbearbeitung und Antragsentscheidung
☒ Auswahl/Beurteilung
☒ Akquise
☒ Auswertungen/Statistiken
☒ Datenweitergabe im Unternehmen
☒ Datenschutzkontrolle, Datensicherung, Sicherstellung eines ordnungsgemäßen Betriebs
☒ Sonstiges: Vertriebs-/Marketingunterstützung."
→I Börse/Makler, 090203/77/2014

Ausführlicher ist die Zweckbeschreibung in der folgenden Vereinbarung. Jedoch wird hier nicht darauf eingegangen, warum die beschriebenen Zwecke nur durch Nutzung einer cloudbasierten Software (hier wiederum zwei Tools von ServiceNow, SaaS- oder PaaS-basiert) erreicht werden können.

„Zweck
Das System dient der Erfassung und Bearbeitung von Supportaufträgen (Complaints) sowie der in den daran anknüpfenden Prozessen Problem Management/Configuration Management/Change Management/Knowledge Management auftretenden Aufgaben (Tasks). Im Einzelnen dient ASSM und eQMS den Zwecken:
– Erfassung und Bearbeitung von ‚Complaints' und ‚Problems'
– Aufbau und Pflege einer Configuration Management Data Base (CMDB)
– Kontrollierte Durchführung und Dokumentation von relevanten Serviceeinsätzen an Kundensystemen
– Bereitstellung eines Web-basierten Serviceportals für die Kunden
– Ermittlung operativer Kennzahlen zu den relevanten Prozessen Erfassung und Bearbeitung von Non-Conformities (NC's)
– Erfassung und Bearbeitung von CAPA's (Corrective And Preventive Actions)
– Bearbeitung des Vigilance Reportings (VR) an Behörden wie z. B. FDA

– Internes und externes Audit Management
– Produktregistrierung

[…]

Die Auswertungen werden genutzt für/um:

– die Einhaltung der Service- und Supportverträge mit unseren Kunden zu gewährleisten
– die Einhaltung der für die involvierten Geschäftsbereiche relevanten Prozesse zu gewährleisten
– das Erreichen von Unternehmenszielen zu ermöglichen bzw. zu kontrollieren
– die Analyse von Kundenzufriedenheit zu unterstützen
– die Analyse von Trends und damit eine Verbesserung von Prozessen und Produkten zu ermöglichen."

→I Anonym, 090203/71/2013

2.2.3 Art der Daten

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Einer der wesentlichen Regelungspunkte hinsichtlich des Datenschutzes sowie hinsichtlich des allgemeinen Persönlichkeitsrechts ist die Benennung der Daten bzw. Datenkategorien, die über Beschäftigte in einem IT-System gespeichert und verarbeitet werden. Um ein Vielfaches mehr ist dies bei cloudbasierter Softwareverwendung der Fall. Denn hierbei sind die Risiken, denen die persönlichen Daten unterliegen, erheblich größer. Ebenso bedürfen die im Folgenden aus den Datenkatalogen gezogenen Auswertungen einer detaillierten Beschreibung. Dies ist nicht zu verwechseln mit der im späteren Regelungspunkt festzulegenden Leistungs- und Verhaltenskontrolle. Die Auswertungskataloge einerseits orientieren sich an der betrieblichen Notwendigkeit, die überhaupt zum Einsatz des Systems führt. Beispielsweise bei einem Zeiterfassungssystem ist der betriebliche Zweck, die Arbeitszeit zu erfassen. Selbstverständlich ist es dann grundsätzlich erlaubt, eine Auswertung hinsichtlich der Arbeitszeit vorzunehmen. Aus den gleichen Daten lassen sich jedoch auch andere Schlussfolgerungen ziehen, beispielsweise, wie oft jemand vergisst,

sich vom System abzumelden und eine Korrekturbitte an den Administrator sendet. Eine Auswertung dahingehend, wie vergesslich ein Mitarbeiter ist, gehört jedoch nicht zur Zweckbestimmung des Systems. Daher hat schon diese Art der Auswertung zu unterbleiben. Dem gegenüber orientiert sich das Maß an zugelassenen Leistungs- und Verhaltenskontrollen ausschließlich daran, ob die Zweckbestimmung des Systems einen mitarbeiterbezogenen Anteil enthält, also überhaupt zu Leistungs- und Verhaltenskontrollen eingesetzt wird. Aus der erfassten Arbeitszeit (Auswertung) darf eine Leistungskontrolle gezogen werden - beispielweise, ob der Mitarbeiter zu viele Überstunden anhäuft. Hier lässt sich also aus der Auswertung (Arbeitszeiterfassung) eine Kontrolle ziehen, die hier zudem auch rechtmäßig wäre. Aber aus anderen, Cloud-basierten Systemen lassen sich zum einen Auswertungen ziehen, die mit dem ursprünglichen Zweck des Systems nicht zu tun haben. Beispielweise könnte aus den Chatinhalten innerhalb eines Cloud-basierten Kommunikationstools geschlossen werden, wie gut sich ein Mitarbeiter in den Regeln der Rechtschreibung auskennt. Da dies jedoch nicht Zweck des Systems ist, hat schon diese Art der Auswertung zu unterbleiben. Dies bedeutet, dass schon, bevor überhaupt an eine Leistungskontrolle gedacht werden könnte, die Daten („Häufigkeit der Schreibfehler“) gar nicht erst erhoben werden dürfen. Zu einer Leistungskontrolle kann es dann mangels Daten gar nicht mehr kommen.

Bei der Benennung der Daten oder Datenkategorien ist zudem entscheidend, wo diese gespeichert werden. Wenn nicht bereits im Gegenstand der Vereinbarung ausführlich darauf eingegangen wurde, welche Software auf der Basis welcher Cloud-Lösung eingesetzt wird, muss dies mindestens hier nachträglich erfolgen. Gleichzeitig muss hinsichtlich aller Daten im Einzelnen der Grund für die Erforderlichkeit der Speicherung und Verwendung angegeben werden.

Fakt ist jedoch, dass dies in den vorliegenden Vereinbarungen ausnahmslos nicht geregelt ist. In einer Vereinbarung zum Spesenabrechnungsmodul Concur ist explizit aufgelistet, welche Daten der Mitarbeiter gespeichert werden.

> „Mitarbeiterdaten:
> – Initialen
> – e-Mail-Adresse
> – Company Code […]
> – Abteilung
> – Adresse
> – Name des Vorgesetzten

und außerdem:
- Country Code (‚DE')
- Kostenstelle
- SAP-HR-Nummer
- Angaben über Freigaberechte als Manager (sofern zutreffend)
- Art der Firmenkreditkarte (sofern zutreffend)
- Nummer der Firmenkreditkarte (sofern zutreffend)
- Ablaufdatum der Gültigkeit der Firmenkreditkarte (sofern zutreffend)
- Daten der abzurechnenden Dienstreise
- Daten der abzurechnenden Promotionsausgaben

[…]

Auswertungen der Mitarbeiterdaten:
- eine nicht-anonyme Auswertung der Mitarbeiterdaten findet nicht statt
- anonyme Auswertungen der Mitarbeiterdaten sind jederzeit zulässig."

→| Großhandel (ohne Kfz.), 090503/43/2009

Zwar wird hier nicht näher bezeichnet, warum genau dieses Datum für die Funktion der Software innerhalb des Unternehmens zwingend Verwendung finden muss, was grundsätzlich dazu führt, dass überhaupt nicht bewertet werden kann, ob das Datum erforderlich ist oder nicht. Im vorliegenden Fall ist ein über die Speicherung hinausgehendes Risiko dadurch gebannt, dass ausschließlich anonymisierte Auswertungen erfolgen sollen. Trotzdem wird übersehen, dass erhebliche Bewegungsdaten der Beschäftigten innerhalb einer cloudbasierten Anwendung vorgehalten werden, die gegebenenfalls Begehrlichkeiten Dritter (z. B. des Cloud-Anbieters) wecken. Denn die Reisebewegungen von europäischen Beschäftigten können für bestimmte Branchen durchaus interessant sein. Ob der zwischen Unternehmen und Cloud-Anbieter bestehende Vertrag, welcher der Datenverarbeitung zugrunde liegt, die Einhaltung der deutschen Datenschutzgesetze ausreichend absichert, kann hier mangels vorliegender Informationen nur vermutet werden.

Die folgende Vereinbarung benennt die Datenkategorien wesentlich ausführlicher.

„Es gibt zwei Arten von Informationen, die im System enthalten sind:

1. Grundlegende Personaldaten
Es gibt ein Basisprofil für jeden User. Die Grundform ist auf den Namen des Mitarbeiters, Personalnummer, Abteilungs-Code, Manager ID und evtl. die Genehmigungsgrenzen beschränkt, wenn die Person ein Genehmiger ist.
2. Transaktionsdaten
Die folgenden Daten werden von der Kreditkarte und dem Nutzer mit der Spesenabrechnung eingereicht:
- Expense Art (z. B. Hotel, Flugkosten etc.)
- Datum der Kosten
- Beträge und Währungen
- Grund für die Kosten, Anmerkungen
- In einigen Fällen können Angaben zur Reiseklasse und zu Ausgangs- und Zielort erforderlich sein. […]

Die ‚Grundlegenden Personaldaten' und ‚Transaktionsdaten' (siehe Ziffer 3.1 und 3.2) werden ausschließlich zur Bearbeitung der Reisekostenabrechnung des jeweiligen Mitarbeiters genutzt und verarbeitet. […] Die Angabe von über die ‚Grundlegenden Personaldaten' und ‚Transaktionsdaten' hinausgehenden weiteren persönlichen Informationen in Concur (Kontaktinformationen für den Notfall und Privatadresse) sind freiwillige Angaben und werden von Concur weder benötigt noch – außer der reinen Speicherung – weiterverarbeitet."

→I Börse/Makler, 090203/76/2014

Es werden hier zwei Datenkategorien getrennt dargestellt, die auch unterschiedlichen Auswertungen unterliegen. Dies entspricht dem Grundsatz der Zweckbestimmung der Daten. Aber auch hier wird wiederum nicht erkannt, dass es einer Begründung bedarf, warum ausgerechnet diese Daten erforderlich sind, um den innerbetrieblichen Zweck des Systems zu erreichen. Warum beispielsweise der Name des Mitarbeiters zusätzlich zu dessen Personalnummer im System erfasst wird, ist nicht ersichtlich. Gerade bei externer Datenverarbeitung wie in einer Cloud wäre es aber zur Risikominimierung sehr sinnvoll, nur die pseudonymisierte Personalnummer zu verwenden. Damit könnten Dritte, die über die Cloud Zugriff auf Daten bekämen, wesentlich weniger Nutzen aus diesen Daten ziehen, weil ihnen die Zuordnungsdatei (Name/Personalnummer) fehlen würde.

Schwierig an diesen Klauseln ist insbesondere, dass zum einen eine freiwillige Datenerfassung ermöglicht werden soll. Die Selbstbestimmung von

Beschäftigten innerhalb eines Unternehmens ist ein datenschutzrechtlich höchst umstrittenes Thema; denn die Freiwilligkeit der Einwilligung ist in einem Über-/Unterordnungsverhältnis zwischen Arbeitgeber und Arbeitnehmer schwer herzustellen. Es kann zumindest nicht gelöst werden, ohne Regelungen in einer Betriebsvereinbarung zu etablieren, die die freiwillige Entscheidung eines einzelnen Beschäftigten unterstützen. Hier müssten zumindest nähere Angaben über das Fehlen jeglicher negativer Konsequenzen für den Fall gemacht werden, dass ein Arbeitnehmer die Angaben verweigert. Insbesondere die Tatsache, dass der Arbeitnehmer vermutlich gar nicht über die Tragweite seiner Entscheidung informiert ist, lässt hier schon jede Einwilligungslösung obsolet werden. Denn solange der Mitarbeiter nicht weiß, dass die Daten vom Unternehmen in eine Cloud „ausgelagert" werden, kann er hierzu keine informierte Entscheidung treffen.

In der folgenden Vereinbarung, die sich wieder mit der cloudbasierten Software Salesforce beschäftigt, wird in größerem Maße versucht, die gesteigerte Überwachungsfähigkeit der cloudgestützten Datenverarbeitung zu reglementieren. Andererseits fehlen jedoch die Angaben zu den genauen Datenkategorien, die hier teilweise nur erahnt werden können.

> „Beide Seiten vereinbaren, die Überwachungseignung des Systems so gering wie möglich zu halten und treffen daher die folgenden Regelungen:
> – Es besteht Einvernehmen, dass das System im Rahmen der Kundenkontakt-Historie nur ausgewählte Ereignisse, z. B. Kundenbesuche, nicht aber zur Erledigung einzelner Arbeitsschritte, verbrauchte Zeiten oder sonstiger Ressourcen erfasst und speichert.
> – Der Mitarbeitername wird dazu verwendet, eine Ansprechperson im Fall von Nachfragen festzulegen. […]
>
> Reporting
>
> Es gilt der Grundsatz, dass die mit Hilfe des Systems erstellbaren Reports dazu verwendet werden, Kundenprojekte effektiv zu verfolgen und voranzutreiben und einen Marktüberblick zu gewinnen um entsprechende strategische Entscheidungen zu treffen. In der Einführungsphase findet in den ersten drei Monaten ein monatliches Review Treffen zwischen Administrator, Geschäftsleitung und Betriebsrat statt. Es werden Reports aus Salesforce.com gezogen und im Review erklärt Anlage 3 Liste aller Reports. […]

> Das Modul ‚Case' (Kundenvorgang) wird in der eingesetzten Version von Salesforce.com nicht benutzt. Somit gibt es keine Messung der Bearbeitungszeit in Salesforce.com auf Mitarbeiter-Ebene."
> ➔ Mess-, Steuer- und Regelungstechnik, 090203/60/2013

In nachstehender Vereinbarung zur gleichen Software wird der Grund für die Aufzeichnung der Datenkategorien bezogen auf Benutzergruppen aufgezeigt. Die Formulierungen „es steht die Vergleichbarkeit von Teams im Vordergrund" und „[relevant] ist die Sichtbarkeit des Nutzungsgrades von Gruppen […] und nicht von einzelnen Benutzern" zeigen zwar, dass eine Beurteilung einzelner Mitarbeiter nicht Sinn und Zweck des Softwareeinsatzes sein soll. Da aber eine Auswertung bezogen auf den Einzelnen nicht kategorisch ausgeschlossen wird, ist dies eine nur wenig effiziente Risikominimierung.

> „Gemäß Anlage 1 zu dieser Ergänzungsvereinbarung kann der allgemeine Nutzungsgrad von Salesforce in Deutschland gemessen werden. Im Vordergrund dabei steht die Vergleichbarkeit von verschiedenen Teams und Funktionen (z. B. Vertrieb, Profit Centers und Standorte), um die Gesamtnutzung und somit auch den Nutzen für den einzelnen Mitarbeiter/innen zu erhöhen.
> […]
> # erstellte Cali Reports
> # erstellte Kontakte
> # Logins
> # erstellte Tasks
> # erstellte Opportunities
> […]
> Folgende Benutzergruppen sollen im Dashboard erfasst werden:
> – Profit Centers
> · Financial Lines
> · Casualty
> · Global Property
> · Specialty
> – Vertrieb mit Standorten:
> · Frankfurt
> · München
> · Hamburg
> · Düsseldorf, Leipzig, Berlin, (Heilbronn) zusammen

- Themenbezogen:
  - MAP Clients
  - z. B. Automotive, Financial Institutions etc.
  - Da Salesforce vom Netzwerkeffekt lebt und sich somit der Nutzen bei breiter Nutzung enorm steigert, ist die Sichtbarkeit des Nutzungsgrades von Gruppen relevant und nicht von einzelnen Benutzern.
- Bei geringer Benutzung von Salesforce (allgemein oder in einzelnen Teams):
  - Zusätzliche Unterstützung dieser Teams
  - Identifikation von Unklarheiten
  - Identifikation von Verbesserungsmöglichkeiten des Systems (dies kann wesentlich zur Weiterentwicklung des Systems beitragen, da wir auf den Input aus dem Kerngeschäft angewiesen sind)
- Bei hoher Benutzung von Salesforce (allgemein oder in einzelnen Teams):
  - Identifikation von weiteren Vorteilen - Gespräche mit den entsprechenden Salesforce Champions, PC Managern, Senior Management und Vertriebsleitern."

→I Börse/Makler, 090203/78/2015

Zu kurz greifen in jedem Fall allgemein gehaltene Aussagen wie in der folgenden Vereinbarung, da nur pauschal „prozessrelevante Kennzahlen", „kundenspezifische Kennzahlen" oder die „involvierten Geschäftsbereiche" genannt werden. Welche Daten diese Kriterien erfüllen und welche nicht, bleibt offen.

„Die Reportinglisten beinhalten Ausweitungen zu/für:
- prozessrelevanten Kennzahlen der involvierten Geschäftsbereiche
- kundenspezifische Kennzahlen, welche in den Service -und Supportverträgen mit unseren Kunden festgeschrieben sind (z. B. Antwort- oder Lösungszeiten für gemeldete Complaints)
- produktspezifische Kennzahlen bzw. Details."

→I Anonym, 090203/71/2013

2.2.4 Zugriffsrechte

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Die Grundsätze des Datenschutzes und der Datensicherheit nach dem BDSG beinhalten auch die in der Anlage zu § 9 benannte Zugriffskontrolle. In der folgenden Betriebsvereinbarung wird wesentlich Wert gelegt auf die systematisch richtige Zuordnung von Verantwortungsbereich und jeweiliger Zugriffsberechtigung. Aber wie auch in den vorherigen Regelungspunkten zeigt die mangelnde Beschäftigung mit der Frage der hinter der Softwarenutzung stehenden Cloudlösung das Problem deutlich auf: Es werden keinerlei Aussagen zu den Zugriffsberechtigten des Cloud-Anbieters getroffen. Je nachdem, welche vertragliche Lösung zwischen Unternehmer und Cloud-Anbieter gefunden wurde, könnte hier eine Lösung vorliegen, die sich im Rahmen der europäischen Gesetze bewegt – oder es könnte ein vollkommen rechtswidriger Vertrag vorliegen. Eine überprüfbare Aussage hierzu macht das hier begutachtete Regelwerk jedenfalls nicht. Denn der Satz „[…] darüber hinaus erfolgt kein Zugriff auf Funktionen und Daten von Concur“ kann sich nicht vollumfänglich auch auf den Cloud-Anbieter beziehen. Denn dieser dürfte sich aller Wahrscheinlichkeit nach zumindest Administratorrechte vertraglich gesichert haben. Es wäre jedenfalls verwunderlich, wenn in einem Unternehmen wie Concur (bzw. jetzt: SAP) kein Administrator derlei weitreichende Zugriffsberechtigungen hätte.

> „Jeder erhält Zugriff auf die Funktionen und Daten von Concur genau in dem Umfang, wie er ihn zur Erledigung seiner Aufgaben im Rahmen der Spesen- und Promotionabrechnung benötigt. Wichtige Einzelheiten bzgl. der Zugriffsberechtigungen sind in Anlage 1 vereinbart; darüber hinaus erfolgt kein Zugriff auf Funktionen und Daten von Concur. […]
> Die Berechtigungsvergabe muss nachvollziehbar und unter Berücksichtigung des Datenschutzes gestaltet und schriftlich dokumentiert sein. […]

Die Systemberechtigten haben uneingeschränkten Zugriff auf alle Daten und Auswertungen für ihren jeweiligen Bereich. […]
Zugriffsberechtigungen
- der Mitarbeiter selbst auf seine eigenen Daten
- der unmittelbare Vorgesetzte des Mitarbeiters, der für die Prüfung und Freigabe der Spesen- und Promotionabrechnung zuständig ist (nur lesend)
- alle Mitarbeiter bzw. Personen, die für die Prüfung und buchhalterische Bearbeitung der Spesen- und Promotionsabrechnung zuständig sind."

→| Großhandel (ohne Kfz.), 090503/43/2009

Wesentlich besser gelungen sind Formulierungen, die sich konkret auf einzelne Standorte und die dortigen, zum Zugriff berechtigten Teams beziehen und tatsächlich auch die Zugriffsberechtigungen des Software-Anbieters beinhalten.

„Der Zugriff ist wie folgt begrenzt:
- Jeder Mitarbeiter hat Zugriff auf seine eigenen Daten.
- [Firma] IT-Personal in der EU, die bei der Überwachung der Datenübertragung beteiligt sind, können bei der Beseitigung von Störungen Daten einsehen.
- [Firma] Personal in [Land], die bei der Prüfung der Reisekosten eingebunden sind, können die Reisekostenabrechnungen einsehen.

[Firma] Mitarbeiter des Concur Support-Teams in [Land] managen die gesamte Systemkonfiguration und haben gegebenenfalls bei Problembeseitigungen Dateneinsicht. Sie stellen ebenfalls auf Anforderung Management-Reports auf dem System bereit. Diese beinhalten Kosten-Analyse von Kosten-Art und/oder Region und alle notwendigen Berichte, die den reibungslosen Ablauf des Systems unterstützen.
- IT-Mitarbeiter des Auftragsdatenverarbeiters Concur Technologies, Inc. […] sind verantwortlich für die Sicherstellung der Datenspeicherung bei dem Dienstleister. Bei Systemproblemen können diese Einsicht in die gespeicherten Daten von Einzelpersonen nur dann nehmen, sofern dies zur Aufrechterhaltung der Funktionsfähigkeit des Systems erforderlich sein sollte.

– [Firma] Finance Mitarbeiter sehen die zusammengefassten Informationen, die der Kreditoren- und Hauptbuchhaltung übergeben werden und der korrekten und pünktlichen Bezahlung dienen."

→I Börse/Makler, 090203/76/2014

Eine gute Lösung ist zudem, auch die vertraglichen Grundlagen für die Auftragsdatenverarbeitung mit dem Software- bzw. Cloud-Anbieter zu benennen. Es empfiehlt sich trotzdem, diese auch explizit – das heißt mit genauer Bezeichnung und Datum – in die Betriebsvereinbarung aufzunehmen. Denn zugrunde liegende Verträge könnten sich ändern und entsprächen dann nicht mehr dem ursprünglichen Vereinbarungsziel.

„Salesforce.com, Inc. hat nur insoweit Zugriff auf personenbezogene Daten als dies für sie zur Erfüllung ihrer Dienstleistungen notwendig oder unumgänglich ist. Dritte sind an strenge vertragliche Rahmenvereinbarungen in Bezug auf Datenverarbeitung gebunden. Der GBR wird über Zugriffsrechte bzw. Datenübermittlung an konzernexterne Dritte informiert."

→I Börse/Makler, 090203/77/2014

Es kann durchaus sinnvoll sein, die Zugriffsberechtigungen durch ein eigenes Managementsystem für das gesamte Unternehmen zu regeln. Trotzdem muss in Bezug auf externe Beteiligte, die wahrscheinlich ihre Berechtigungen nicht über dieses System zugewiesen bekommen, eigens eingegangen werden. Andernfalls bestehen erhebliche Wissenslücken bei der Frage: Wer kann in welchem Umfang beispielsweise Kundenbeschwerden einsehen? Dies ist etwa nachstehend bei der Nutzung eines cloudbasierten elektronischen Qualitätsmanagement-Systems der Fall.

„Das Antrags- und Freigabeverfahren für Berechtigungs- und Rollenänderungen wird über das global eingesetzten User Administration Tool (UAT) incl. Approval-Workflow durchgeführt."

→I Anonym, 090203/71/2013

2.2.5 Verknüpfungen mit anderen Systemen, Schnittstellen

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Bei cloudbasierten Softwareanwendungen wäre zu erwarten, dass gerade auf die Verknüpfung von unterschiedlichen Systemen ausführlich und ausdrücklich eingegangen wird. Tatsächlich enthalten jedoch nur drei der ausgewerteten Vereinbarungen überhaupt eine Aussage hierzu. Wie und in welchem Maße bei den unterschiedlichen cloudgestützten Softwareanwendungen Schnittstellen zu anderen Programmen existieren, kann nicht allgemein beantwortet werden. Es ist zu vermuten, dass zumindest erheblich mehr Möglichkeiten bestehen, als in den Vereinbarungen genannt werden.

> „Es ist nicht beabsichtigt, Schnittstellen mit anderen Systemen herzustellen."
> →I Börse/Makler, 090203/77/2014

Die folgenden beiden Vereinbarungstexte beziehen sich auf die gleiche Anwendung und zeigen, wie unterschiedlich mit der Frage nach den vorhandenen Datenwegen umgegangen wird. Geht man davon aus, dass sich auch die Vereinbarung aus dem Jahr 2009 mittlerweile auf eine cloudbasierte Software bezieht (weil das Unternehmen Concur/SAP nur noch diese anbietet), ist die folgende Formulierung wesentlich realitätsnäher als die vorhergehende.

> „Schnittstellen zu anderen IT-Systemen bzgl. Mitarbeiterdaten:
> – folgende Daten werden an [die Firma] zum Zwecke der Auszahlung und Verbuchung übergeben:
> Initialen, Kostenstellen, Kostenarten) Angabe zur Umsatzsteuer, zu erstattende Beträge, Buchungstexte."
> →I Großhandel (ohne Kfz.), 090503/43/2009

Nur in einer der Vereinbarung ist ausführlich beschrieben, welche Wege die gespeicherten Daten nehmen.

„Die Daten werden an drei Stellen gespeichert, wenn sie durch das System fließen:

- Die Daten werden von den lokalen HR und Finanzsystemen zur Verfügung gestellt und in der Gemeinsamen Europäischen Demografischen Data Base (CDDB) gespeichert. Diese Datenbank in [Land] dient der Sammlung der Daten zur Weiterleitung an das Verarbeitungssystem.
- Die Daten werden via SFTP zur Verschlüsselung an die [Firma] [Land] gesandt, bevor sie von dort über SFTP an das Concur-System in [Land] übertragen werden. Die Daten werden in diesem System maximal zwei Tage gehalten, da es lediglich der Verschlüsselung und Übertragung der Daten an Concur dient.
- Abrechnungsdetails werden direkt in das Concur-System über das Internet verschlüsselt eingegeben und als work in progress zwischengespeichert, bis die Spesenabrechnungen zur Zahlung freigegeben werden. Die genehmigten Ausgaben werden als Zusammenfassung an [die Firma] über den internationalen Zugang zurückgesandt und auch im Concur-System archiviert. Diese Archivierung dient Prüfungs- und Steuerzwecken und die Dauer richtet sich nach den gesetzlichen Anforderungen (derzeit 7 Jahre).“

→| Börse/Makler, 090203/76/2014

2.2.6 Aufbewahrungsfristen, Löschfristen

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Wesentlich für den Regelungspunkt Löschfristen in Betriebsvereinbarungen ist die Tatsache: Das deutsche Datenschutzrecht geht gemäß § 35 BDSG im Regelfall davon aus, dass Daten zu löschen sind, soweit nicht gesetzliche oder vertragliche Aufbewahrungsfristen oder schutzwürdige Belange der bzw. des Betroffenen dem entgegenstehen. Im Beschäftigungsverhältnis besagt § 32 BDSG, dass Daten von Arbeitnehmern nur für den Beginn, die Durchführung oder die Beendigung eines Arbeitsverhältnisses gespeichert werden dür-

fen und zu löschen sind, wenn diese Gründe nicht mehr vorliegen. Bei den hier in Rede stehenden Cloud-Anwendungen, die vornehmlich der Aufrechterhaltung des Geschäftsbetriebs eines Unternehmens dienen, sind also die dort gespeicherten Beschäftigtendaten zu löschen, soweit es nach § 32 BDSG hierfür keine Rechtfertigung mehr gibt. Dies wird sich in den meisten Fällen an dem Prüfungspunkt „Durchführung des Beschäftigungsverhältnisses" orientieren müssen. Wenn und soweit Daten der Beschäftigten, wie z. B. beispielsweise Abrechnungsdaten bei Reisekosten-Tools, noch zur Durchführung des Arbeitsverhältnisses erforderlich sind, dürften diese grundsätzlich vorgehalten werden. Wie lange dies aber genau der Fall ist, muss explizit in der Vereinbarung benannt und begründet werden. Hier können beispielsweise Aufbewahrungsfristen aus Steuergesetzen benannt werden, die das Unternehmen verpflichtet, die Daten mehrere Jahre aufzubewahren.

In den vorliegenden Vereinbarungen kommen diese Fristen entweder gar nicht vor oder werden sehr verkürzt angegeben. Eine pauschale Aussage, dass Daten gelöscht werden, soweit der zugrunde liegende Verwendungszweck nicht mehr vorliegt, ist lediglich die Wiederholung der Gesetzeslage und bei Weitem zu ungenau.

> „Mitarbeiterdaten werden nur solange gespeichert, wie der zugrunde liegende Verwendungszweck dies erfordert. Entfällt der Verwendungszweck, sind sie unverzüglich zu löschen oder zu anonymisieren."
>
> → Großhandel (ohne Kfz.), 090503/43/2009

Idealerweise werden Fristen genau benannt. In den folgenden zwei Vereinbarungen wird die Löschung von Daten auf unterschiedliche Weise gewährleistet: In der ersten Betriebsvereinbarung wird auf eine „schriftliche Vereinbarung" verwiesen, nach der die Daten gelöscht werden müssen. Man kann vermuten, dass hiermit ein Vertrag mit dem Auftragsdatenverarbeiter, gegebenenfalls also mit dem Cloud-Anbieter gemeint ist, der konkrete Löschfristen vorsieht. In der zweiten Betriebsvereinbarung ist geregelt, dass die Daten offenbar einem Löschkonzept des Unternehmens unterliegen. Beides ist in der jeweils vorliegenden Vereinbarung jedoch zu unkonkret formuliert, wenngleich die Ansätze gut sind. Richtiger wäre es hier gewesen, sowohl die schriftliche Vereinbarung als auch das Löschkonzept genau zu benennen.

„Löschungsfristen
☒ Gesetzliche Aufbewahrungsfristen: 7 Jahre bzw.
☒ Die Daten werden gelöscht, sobald der Zweck der Daten nicht mehr besteht. […]
Wie wird gewährleistet, dass nach Ablauf der Aufbewahrungsfrist eine Löschung erfolgt? Schriftliche Vereinbarung."
➔ Börse/Makler, 090203/76/2014

„Löschungsfristen
☒ Aufbewahrungsfrist: 4 Jahre
☒ Die Daten werden gelöscht, sobald der Zweck der Daten nicht mehr besteht. […]
Wie wird gewährleistet, dass nach Ablauf der Aufbewahrungsfrist eine Löschung erfolgt? Löschkonzept."
➔ Börse/Makler, 090203/77/2014

2.2.7 Grenzüberschreitender Datenverkehr, Konzerndatenfluss, Auftragskontrolle

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Wie in Kapitel 1 geschildert, haben sich die rechtlichen Grundlagen für den internationalen Datenaustausch seit dem Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 schlagartig verändert. Verständlicherweise nehmen jedoch die hier vorliegenden Vereinbarungen teilweise auf Safe Harbor Bezug. Nun zeigt sich, dass es ein Fehler war, sich auf diese bereits früher in die Kritik geratene Zertifizierung zu verlassen. Vereinbarungen, die sich alleine hierauf stützen, entbehren nun jeglicher Rechtfertigungsgrundlagen für die Datenübermittlung in Staaten ohne ausreichendes Datenschutzniveau.

Der generelle datenschutzrechtliche Hintergrund ist folgender: Wollen Unternehmen ihre Beschäftigtendaten durch externe Dritte verarbeiten lassen, so ist dies nur durch Abschluss eines sogenannten Auftragsdatenverarbeitungsvertrags gemäß § 11 BDSG möglich. Dies gilt schon für eine Auslagerung der Datenverarbeitung innerhalb Deutschlands oder innerhalb Euro-

pas. Umso mehr müssen externe Datenverarbeitungen, die in Staaten ohne angemessenes Datenschutzniveau stattfinden, abgesichert werden. Hierzu gibt bzw. gab es mehrere Alternativen. Zusätzlichen zu den nach § 11 BDSG verpflichtenden Auftragsdatenverarbeitungsverträgen konnten die Unternehmen entweder mit externen Dienstleistern zusammenarbeiten, die nach dem Safe Harbor abkommen zertifiziert waren; oder sie konnten in eigens dafür entwickelten Codes of Conduct mit dem (konzerninternen) Dienstleister vertraglich festlegen, dass europäische Datenschutzstandards eingehalten werden. Eine weitere und generell zu bevorzugende Möglichkeit stellte der Abschluss der sogenannten EU-Standardvertragsklauseln zwischen den Beteiligten dar. Diese, von der EU-Kommission entwickelten Verträge beinhalteten alle Regelungen, die für den internationalen Datentransfer vonnöten waren. Viele Unternehmen griffen jedoch lieber auf die Safe Harbor Lösung zurück, weil diese vermeintlich einfacher umzusetzen war – musste sich ein Unternehmen doch nur einmalig beim US-Handelsministeriums zertifizieren lassen. Dahingegen muss der Abschluss der EU-Standardvertragsklauseln grundsätzlich für jede Geschäftsbeziehung einzeln abgeschlossen werden. Nun hat der EuGH diese Möglichkeit gestoppt, so dass Unternehmen nur noch auf die beiden anderen Alternativen zurückgreifen können. Und auch diese stehen zurzeit in der Kritik. Zumindest an der Frage der Ungültigkeit des Safe-Harbor-Abkommens werden einige der abgeschlossenen Vereinbarungen nun scheitern und müssen neu gefasst werden.

Die folgende Vereinbarung fußt ausschließlich auf dem Safe-Harbor-Zertifikat. Aus der Vereinbarung ist zudem nicht ersichtlich, welche Rolle die so benannte „xy-Corporation“ spielt (die nicht mit dem Arbeitgeber identisch ist). Sie transferiert offenbar personenbezogene Daten in die USA oder ist zumindest daran beteiligt. Die im Zitat genannte Safe-Harbor-Zertifizierung bezieht sich auf diesen Dienstleister. Der Hinweis dieses Dienstleisters „Do You Agree to Corporate and Comply with the EU and/or Swiss Data Protection Authorities? Yes“ müsste nun vom Mitbestimmungsgremium überprüft werden. Denn die deutschen Aufsichtsbehörden können die Safe-Harbor-Zertifizierung nach dem EuGH-Urteil nicht mehr gelten lassen. Über die Zertifizierung der Cloud als solche (in diesem Fall Salesforce) ist in dieser Vereinbarung jedoch nichts zu lesen. Aus Sicht des Betriebsratsgremiums kann nur vermutet werden, dass diese Datenübertragung rechtmäßig abläuft.

> „Daten dürfen außerhalb der EU nur gesehen werden, wenn eine gültige Safe Harbor Vereinbarung vorliegt, wie im Beispiel Anlage 2.

Anlage 2:
Safe Harbor Information:
Original Certification: [Datum]
Next Certification: [Datum]
Personal Information Received from the EU/EEA and/or Switzerland:
Xy-Corporation will use and otherwise process European employee data in the United States for the following purposes (1) to administer and manage its professional development and performance program; (2) to administer and manage its integrity and compliance training program; (3) to maintain and manage the myXy-database, a basic source of personal data for other company applications; and (4) to manage its Helpline (employee reporting hotline).
Privacy Policy Effective- 4/1/2011
Location: http://www.xy-.com/terms
[…]
Privacy Programs: none
Verification: self-assessment compliance review
Dispute Resolution: EU data protection authorities
Personal Data covered: European employee data
Organisation Human Resource Data Covered: Yes
Do You Agree to Corporate and Comply with the EU an/or Swiss Data Protection Authorities? Yes
Relevant Countries from which Personal Information is Received: Austria, Belgium, Denmark, Germany, Ireland, Italy, Spain, United Kingdom."

→| Mess-, Steuer- und Regelungstechnik, 090203/60/2013

Wesentlich ausführlicher und daher nachvollziehbarer löst die folgende Betriebsvereinbarung das Problem des internationalen Datenverkehrs. Sie bezieht sich auf die gleiche Cloud-Lösung. Zum einen wurden hier neben Safe Harbor zusätzlich die EU-Standardvertragsklauseln (die sogenannten Model Clauses) als Rechtfertigungslösung bevorzugt, die zumindest zurzeit nicht direkt vom EuGH-Urteil betroffen sind. Zum anderen wurden die vertraglichen Grundlagen der Datenübertragung exakt mit Abschlussdatum benannt. Und dies sowohl in Bezug auf den Auftragsdatenverarbeitungsvertrag nach § 11 BDSG (siehe „Auftragskontrolle") als auch auf die EU-Standardvertragsklauseln. Diese sind im Übrigen auch aktuell, da nach dem 5.10.2010 nur noch die neuen Klauseln (mit diesem Datum) genutzt werden dürfen. Wie

man hier gut sehen kann, ist hier innerhalb einer Betriebsvereinbarung auch die adäquate Stelle, an der die sonstigen Zertifizierungen, z. B. diejenigen nach DIN-Normen, erwähnt werden können.

> „[Die Firma] hat sich entschieden, bestimmte Aufgaben an externe Dienstleister zu vergeben, so dass bestimmte persönliche Mitarbeiterinformationen an bestimmte sorgfältig ausgewählte, Dienstleister und verbundene Unternehmen der [Firma] übertragen werden. Um den ordnungsgemäßen Austausch von Daten zwischen seinen weltweiten Unternehmen und nicht-verbundenen Dritt-Dienstleistern sicherzustellen, hat [die Firma] folgende Vorkehrungen getroffen: […].
> Die Europäische Kommission hat Standardvertragsklauseln genehmigt, auch bekannt als ‚Model Clauses', die den Export von personenbezogenen Daten von einem im EWR [Europäischen Wirtschaftsraum] ansässigen Datenverantwortlichen zu einem Datenverarbeiter oder einem anderen Datenverantwortlichen außerhalb des EWR regeln. Diese Model Clauses sind, neben anderen Regelungen zu speziellen Datenschutzvorgaben außereuropäischer Jurisdiktionen, in einem ‚Inter-Affiliate Data Transfer Agreement' [DTA], das von allen betroffenen verbundenen Unternehmen der [Firma] unterzeichnet wurde, niedergelegt. Die Anwendung dieser Model Clauses bietet für die übertragenen Daten einen angemessenen rechtlichen Schutz. Das […] Europe Compliance Program gründet auf einem Netzwerk von Musterklauseln und, soweit einschlägig, auf anderen rechtlichen Ausnahmen. […]
> Salesforce.com, Inc. selbst hat ein Safe Harbour Certificate sowie eine Vereinbarung zur Datenübertragung, die den europäischen Standards entspricht, unterzeichnet. […]
> Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können:
> ☒ Öffentliche Stellen bei Vorliegen einer vorrangigen Rechtsvorschrift
> ☐ Andere externe Stellen
> ☐ Nur interne Stellen bei der verantwortlichen Stelle
> ☒ Externe Stellen im Konzern
> ☒ IT-Dienstleister
> ☐ Andere Dienstleister
> ☐ Weitere Empfänger:

[…]
Geplante Datenübermittlung in Drittstaaten (Staaten außerhalb der EU)
☐ Nicht geplant
☐ Sicheres Drittland
☒ USA
  ☒ Save Harbour
  ☐ Standard Vertragsklauseln (extern)
  ☐ Sonstige Verträge (extern)
☒ Standard Vertragsklauseln (intern [Firma] Interaffiliate DTA vom [Datum])
[…]
Auftragskontrolle
Maßnahmen zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer
☒ Vertrag vorhanden (vom [Datum])
☒ Schriftliche Weisungen erteilt
☒ Formalisierte Auftragserteilung vorhanden
☒ Kriterien zur Auswahl beachtet
☒ Erfolgt eine protokollierte Kontrolle beim Auftragnehmer."
→I Börse/Makler, 090203/77/2014

Problematisch bleibt trotz der ausführlichen Beschreibung, dass die Vereinbarung auch an anderer Stelle nicht auf die Tatsache eingeht, dass es sich um cloudbasierte Anwendungen handelt. Dies bedeutet, dass der Betriebsrat trotz der abgeschlossenen Verträge zur Datenverwendung in unsicheren Drittstaaten kaum überprüfen kann, ob sich alle Beteiligten an die Verträge und die bestehenden Gesetze halten. Der Grund hierfür ist einfach: mangels Benennung aller Beteiligten. Die Erfahrung zeigt, dass die meisten Gremien heute noch unsicher sind in Fragen der konkreten Datenverarbeitung und der damit verbundenen Datenströme. Werden sie nicht im Vorfeld geklärt, erzeugt dies später erhebliche Schwierigkeiten, wenn Fragen zu den genauen Wegen auftauchen, die die Daten im weltweiten Netz nehmen. Den meisten Gremiumsmitgliedern dürfte weder durch die Vorarbeiten noch beim Abschluss der Betriebsvereinbarung bewusst geworden sein, dass die persönlichen Daten der Mitarbeiter auf weltweit verteilten Servern liegen (könnten). Um es noch deutlicher zu sagen: Die Daten, auf die sich die Betriebsvereinbarung aus dem Jahr 2014 bezieht, könnten genauso gut in der EU gespeichert werden, da der Cloud-

Anbieter bereits 2013 sein europäisches Datenzentrum plante. Genau wissen können die Mitarbeiter dies hingegen nicht – es ist nirgendwo explizit erklärt.

Einen weiteren Lösungsversuch zeigt die folgende Betriebsvereinbarung. Auch er greift jedoch leider zu kurz. Zwar werden gut durchdachte Kontrollrechte des Gremiums mit der Frage der ausgelagerten Datenverarbeitung verknüpft: Beispielsweise wird reglementiert, dass eine Datenweitergabe nur in bestimmten Fällen erlaubt ist und der Betriebsrat hierüber umgehend zu informieren ist. Was jedoch fehlt, ist die durch den Betriebsrat nachprüfbare Konkretisierung insbesondere bei der Auslandsdatenverarbeitung. Besser ist es, im Vorfeld die Gültigkeit der Vereinbarung davon abhängig zu machen, dass dem Betriebsrat die entsprechenden – unterzeichneten! – Verträge vorab zur Kenntnis gebracht werden. Dies entspricht der Informationspflicht des Unternehmens aus § 80 Abs. 2 BetrVG und sollte nicht in eine Holschuld des Gremiums umgewandelt werden.

> „Eine Übermittlung von Mitarbeiterdaten an Dritte ist nur bei durch Tatsachen begründeten Verdachtsfällen einer strafbaren Handlung und nur insoweit zulässig, als diese Dritten mit der Aufklärung und Verfolgung strafbarer Handlungen befasst sind; Voraussetzung dafür ist, dass vorher das in IV beschriebene Verfahren durchgeführt wurde. Der Betriebsrat wird über die eventuelle Übermittlung umgehend und umfassend informiert.
> Falls die Mitarbeiterdaten im Ausland verarbeitet oder genutzt werden, weist die [Firma] dem Betriebsrat nach, dass dabei die gesetzlichen Datenschutzbestimmungen eingehalten werden. […]
> Die Informations-, Mitbestimmungs- und Kontrollrechte des Betriebsrats und die individuellen Rechte der Mitarbeiter dürfen nicht dadurch beeinträchtigt werden, dass Concur ganz oder teilweise im Auftrag der [Firma] durch andere Personen oder Firmen betrieben wird. Falls erforderlich, werden diese Rechte bei der Gestaltung der Verträge für die Auftragsdatenverarbeitung bzw. Funktionsübertragung entsprechend berücksichtigt. Auf Verlangen gewährt die [Firma] dem Betriebsrat Einsicht in die entsprechenden Vertragsbestimmungen."
>
> →I Großhandel (ohne Kfz.), 090503/43/2009

Abschließend sei zu diesen Regelungspunkt angemerkt: Mitbestimmungsgremien sollten sich stets darüber im Klaren sein, dass sie an diesem Punkt ei-

nem gewissen Dilemma unterliegen: Sie sollen nach § 80 Abs. 1 Nr. 1 BetrVG darüber wachen, dass der Arbeitgeber die zum Schutz der Beschäftigten geltenden Vorschriften einhält – haben hierzu aber kein „scharfes Schwert" an der Hand. Sie können dies nicht gerichtlich durchsetzen, sondern nur im Wege der vertrauensvollen Zusammenarbeit mit der Arbeitgeberseite darauf hinwirken. Das schafft das Problem, dass der Betriebsrat im Grunde genommen keine Handhabe hat, wenn in der Betriebsvereinbarung auf den Abschluss entsprechender internationaler Verträge (EU-Standardvertragsklauseln oder Ähnliches) hingewiesen wird. Sind diese Verträge allerdings (noch) nicht abgeschlossen, kann sich das Gremium lediglich an seinen Unternehmer wenden, um dies voranzutreiben. Gegenüber dem externen Datenverarbeiter hat er keinerlei Rechte. Sinnvoll ist es daher, das Wirksamwerden entsprechender Betriebsvereinbarungen von der Tatsache und dem Datum des Vertragsschlusses zwischen Arbeitgeber und externem Datenverarbeiter abhängig zu machen. So behält der Betriebsrat – qua zwingenden Mitbestimmungsrechts – noch die Möglichkeit, die (Betriebsvereinbarungs-)Verhandlungen für gescheitert zu erklären und weitere rechtliche Schritte zu unternehmen, falls die entsprechenden internationalen Verträge aus irgendeinem Grund nicht zustande kommen.

2.2.8 Leistungs- und Verhaltenskontrollen

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Ein Regelungspunkt ist sowohl betriebsverfassungsrechtlich als auch datenschutzrechtlich von großer Bedeutung: Die Ausgestaltung der Leistungs- und Verhaltenskontrollen in Betriebsvereinbarungen. Betriebsverfassungsrechtlich kann hier das in § 87 Abs. 1 Nr. 6 BetrVG normierte, zwingende Mitbestimmungsrecht bei technischen Verfahren, die zur Überwachung der Mitarbeiter geeignet sind, ausgestaltet werden. Datenschutzrechtlich ist ein Arbeitgeber verpflichtet, bei nicht zwingend erforderlicher Datenverarbeitung von Beschäftigtendaten eine rechtfertigende Norm zu schaffen, die die Datenverarbeitung legitimiert. § 4 Abs. 1 BDSG sieht vor, dass auch eine „andere

Rechtsvorschrift“ als Rechtfertigungsgrundlage ausreichend ist. Die Qualität einer solchen anderen Rechtsvorschrift erreicht eine Betriebsvereinbarung aufgrund ihres (teilweise) normativen Charakters. Auf der Basis der unter diesem Regelungspunkt festgelegten Grundsätze zur Leistungs- und Verhaltenskontrolle kann dann an späterer Stelle auch die Verwertung der so erlangten Informationen näher bestimmt werden. Wichtig sind hierbei insbesondere Beweisverwertungsverbote, die sich auf zu Unrecht erhobene Daten beziehen müssen.

Richtig erkannt haben viele Gremien, dass dieser Regelungspunkt ausführlich und detailliert zu behandeln ist, wenn es um Überwachungsrisiken geht, die dem Arbeitgeberwunsch nach umfassenden Kontrollen entspringen. Auch die Abläufe minutiös darzulegen, die zu einer Verwendung der Daten insbesondere bei strafrechtlich relevantem Verhalten führen können, wurde richtig erkannt. Dies entspricht dem Verhältnismäßigkeitsgrundsatz bei der gegenseitigen Grundrechtsabwägung von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (Allgemeines Persönlichkeitsrecht und Recht auf informationelle Selbstbestimmung der Arbeitnehmer) und andererseits von Art. 12 GG (Recht des Arbeitgebers auf Durchführung seiner unternehmerischen Tätigkeit).

> „Eine Verhaltens- oder Leistungskontrolle der Mitarbeiter oder von überschaubaren Gruppen von Mitarbeitern im Sinne von § 87 Abs. 1 Nr. 6 BetrVG durch Concur ist nur in Bezug auf Rechtzeitigkeit, Vollständigkeit oder Richtigkeit von Spesen- oder Promotionsabrechnungen der Mitarbeiter zulässig. Bei nicht ordnungsgemäßer Spesen- und Promotionabrechnung wird die Abrechnung im Sinne einer vertrauensvollen Zusammenarbeit an den Mitarbeiter zurückgeschickt und es soll ggf. ein klärendes Gespräch zu den festgestellten Abweichungen geführt werden, um festzustellen, ob es sich ggf. um einen Irrtum oder ein falsches Verständnis der Reisekostenrichtlinie handelt, das durch eine Erklärung bzw. Schulung für die korrekte Erstellung zukünftiger Abrechnungen vermieden werden kann.
> Unberührt davon bleibt die Möglichkeit der [Firma], Concur zur Aufklärung und Verfolgung von durch Tatsachen begründeten Verdachtsfällen einer strafbaren Handlung zu nutzen. Liegen entsprechende Tatsachen vor, werden sich Vertreter der [Firma] und des Betriebsrats unverzüglich zu einem klärenden Gespräch zusammensetzen. Ziel dieses Gesprächs ist es zu prüfen, ob sich der Verdacht einer strafbaren Handlung aufrechterhalten lässt.

> Sollte nach diesem Gespräch aus Sicht der [Firma] nach wie vor der Verdacht einer strafbaren Handlung bestehen, muss ein Gespräch mit dem Mitarbeiter geführt werden. Der Mitarbeiter kann zu diesem Gespräch ein Mitglied, des Betriebsrates und/oder eine andere Person seines Vertrauens hinzuziehen; der Mitarbeiter ist hierauf hinzuweisen. Der Mitarbeiter wird zu diesem Gespräch, schriftlich unter Angabe der Verdachtsmomente und unter Vorlage der entsprechenden Unterlagen mit 3-Tagesfrist eingeladen. Danach kann [die Firma] entsprechende arbeitsrechtliche oder strafrechtliche Maßnahmen in die Wege leiten, ansonsten ist das Verfahren damit beendet."
>
> ➔ Großhandel (ohne Kfz.), 090503/43/2009

Wenngleich ein Arbeitgeber grundsätzlich keine Strafverfolgungsbehörde ist, entspricht die Formulierung „[…] Concur zur Aufklärung und Verfolgung von durch Tatsachen begründeten Verdachtsfällen einer strafbaren Handlung zu nutzen" in etwa dem Wortlaut des § 32 Abs. 1 Satz 2 BDSG. Hierbei ist wichtig, dass die Tatsachen, die durch eine Verwendung von Daten aus dem System untermauert werden sollen, im Vorfeld bestehen und nicht erst durch die Verwendung der Daten aus der Abrechnungssoftware heraus entstehen.

Da jedoch in keiner der Vereinbarungen die Cloud-Datenverarbeitung konkret benannt wird, fällt es hier schwer, die konkreten Informationen aufzulisten, die zwischen Arbeitgeber und Cloud-Anbieter fließen oder zumindest fließen könnten. Dies wäre jedoch zur Darlegung und einer folgenden, konkreten Eingrenzung der Risiken erforderlich. Grundsätzlich sind viele Gremien der Meinung, dass eine detaillierte Aufschlüsselung aller vorhandenen Möglichkeiten der Leistungs- und Verhaltenskontrolle dann nicht notwendig ist, wenn diese in der Betriebsvereinbarung weitgehend ausgeschlossen wurde. Dies kann jedoch nicht dem Gebot der Transparenz entsprechen. Betriebsräte verlassen sich zu sehr auf umfängliche Ausschlussklauseln ohne genau zu wissen, welche Möglichkeiten der Überwachung sich überhaupt in einem System „verstecken". Es entspricht langjähriger Erfahrung, dass tatsächlich nur durch die konkrete Beschreibung aller vorhandenen Kontrollmöglichkeiten ein Ausschluss derselben überhaupt greift. Vermutlich entspricht es der menschlichen Natur, Risiken erst einschätzen zu können und Risikofolgen erst dann wirklich zu erfassen, wenn diese verständlich und konkret und nicht nebulös und verallgemeinert dargestellt werden.

Das Problem ist jedoch vor allem unter dem Aspekt der schwierigen Urteilslage hinsichtlich wirksamer Beweisverwertungsklauseln zu betrachten:

Ein pauschaler Ausschluss jeglicher Verwendung wird voraussichtlich von einem Gericht nicht anerkannt werden. Was also aufgrund der Totalität eines Verwertungsausschlusses vermeintlich die größte Sicherheit bringen soll, erschafft am Ende das genaue Gegenteil. Spätestens, wenn vom Cloud-Anbieter an den Arbeitgeber Daten übermittelt werden, mit denen der Betriebsrat nicht gerechnet hat, wird die Frage laut, ob genau diese Datenkategorie überhaupt vom Ausschluss umfasst sein sollte.

Das letzte Beispiel, das in der Fortsetzung der Vereinbarung weitere problematische Klauseln enthält, zeigt dies deutlich. Es wird zwar sehr ausführlich auf alle möglichen Datenauswertungsmöglichkeiten eingegangen und es wird versucht, die Leistungs- und Verhaltenskontrollen weitreichend auszuschließen. Da jedoch in früheren Gliederungspunkten der Vereinbarung nicht darauf eingegangen wurde, wie genau die vertragliche Vereinbarung zwischen Cloud-Anbieter und Arbeitgeber aussieht, fehlt hier beispielsweise ein wesentlicher Punkt: die Abrechnungsdaten. Wenn und soweit ein Cloud-Anbieter nach Volumentarifen abrechnet, wird die Verwendung der Volumina im Unternehmen, bezogen auf einzelne IP-Adressen oder Client-Zugänge oder Ähnliches, möglicherweise einzelnen Mitarbeitern zuzuordnen sein. Stellt der Cloud-Anbieter sie dem Arbeitgeber zur Verfügung, kann dies hervorragend zu Leistungs- und Verhaltenskontrollen verwendet werden. Falls hier später Kündigungswellen die vermeintlichen „Low-Performer“ treffen, wird schwer nachzuweisen sein, woher die Informationen stammen. Beschäftigte könnten in Verdacht geraten, weniger zu leisten, wenn ihr Volumenverbrauch geringer ausfällt. Sie könnten auch in den Verdacht geraten, zu langsam zu arbeiten, wenn ihre Zugriffszeiten vom Durchschnitt der Belegschaft nach oben abweichen. Da hierüber nichts Genaues in der Vereinbarung geregelt ist, kann der Betriebsrat nur Vermutungen anstellen, ob solche Daten dem Arbeitgeber vorliegen.

> „Mitarbeiterbezogene Systemdaten (z. B. Systemanmeldedaten, interne Protokollierungen, Benutzerstatistiken), die aus technischen Gründen erforderlich sind, dürfen, soweit in dieser Betriebsvereinbarung nichts anderes geregelt ist, nur für technische Zwecke (Steuerung und technische Optimierung der Systeme), zur Gewährleistung der Systemsicherheit, für Zwecke der Revision und zur Kontrolle des Datenschutzes und dieser Betriebsvereinbarung und nur von den Personen, die dafür zuständig sind, verarbeitet oder genutzt werden. Die Systemberechtigten sind zur Verschwiegenheit auch gegenüber Vorgesetzten verpflichtet, falls sie auf Erkenntnisse stoßen, die

> Rückschlüsse auf das Verhalten oder die Leistung von Mitarbeitern ermöglichen. Von der Verschwiegenheitsverpflichtung ausgenommen sind Erkenntnisse, die strafrechtlich relevant sein könnten. In diesem Falle wird der Betriebsrat umgehend darüber unterrichtet. Werden die Systemberechtigten durch Vorgesetzte angewiesen, gegen diese Betriebsvereinbarung zu verstoßen, so dürfen sie dieser Anweisung nicht Folge leisten. […]
> Alle personellen Maßnahmen der [Firma] zum Nachteil eines Mitarbeiters, die auf Informationen beruhen, die unter Verstoß gegen diese Betriebsvereinbarung gewonnen wurden, sind von vornherein unwirksam. Das gilt auch dann, wenn diese Informationen durch firmenfremde Personen oder Firmen ermittelt und der [Firma] zur Kenntnis gebracht wurden."
> ➔I Großhandel (ohne Kfz.), 090503/43/2009

Zu unbestimmt ist hier die Formulierung der Ausnahmen: Mitarbeiterbezogene Systemdaten dürfen zwar grundsätzlich nur für technische, revisionsbezogene oder Datenschutzkontrollzwecke verwendet werden, aber auch für Zwecke „der Kontrolle […] dieser Betriebsvereinbarung". Besser wäre es hier, genau festzulegen, welche Daten für welche Leistungs- oder Verhaltenskontrollen Verwendung finden dürfen. Dies ist zugegebenermaßen aufwendiger, lässt später aber weniger Interpretationsspielraum zu. Es empfiehlt sich an dieser Stelle, auf die möglichst vorher in der Vereinbarung konkret benannten Auswertungsmöglichkeiten Bezug zu nehmen und daran die Kontrollmöglichkeiten zu orientieren. Es kann dabei beispielsweise auf bestimmte Reports, die über die Software erstellt werden können, hingewiesen werden. Dann ist auch klargestellt, dass nur diese Report-Generierung sowohl für die Arbeitgeberseite als auch für den Cloud-Anbieter selbst erlaubt ist.

Gut gelöst ist hierbei die ausführliche Darlegung dessen, was Systemberechtigte, die stets weiterreichenden Zugriff auf Daten haben als alle anderen Berechtigten, aus dem System auswerten dürfen. Insbesondere der Hinweis, dass sie nicht von Vorgesetzten angewiesen werden dürfen, gegen die Betriebsvereinbarung zu verstoßen mag seltsam anmuten. Dies könnte als die Unterstellung von bereits im Vorfeld geplanten Verstößen gegen die Vereinbarung ausgelegt werden. Es entspricht jedoch oft der Realität, dass – und sei es aus Unwissen – gerade Systemverantwortliche gebeten werden, mehr Informationen aus einem System zu ziehen, als es erlaubt ist. Problematisch ist hier allerdings, dass die Betriebsvereinbarung dies nur für unternehmensangehörige Systemverantwortliche des Arbeitgebers regeln kann. Ob in den

Verträgen zwischen Arbeitgeber und Cloud-Anbieter gleichlautende Klauseln genutzt wurden, um auch Systemverantwortliche des externen Anbieters zu verpflichten, kann nur vermutet werden. Diese Verpflichtungsklauseln sind umso wichtiger, als sie sich auf alle Systemverantwortlichen beziehen müssen, die an allen einbezogenen Servern – welche bei Auftragsspitzen gegebenenfalls weltweit hinzugebucht werden – auf die Daten des Unternehmens zugreifen können. Denn das ist gerade der Vorteil einer cloudgestützten Datenverarbeitung: dass die Nutzung von Ressourcen sich am abgefragten Volumen orientieren kann. Wie die Verteilung in Zeiten überproportionaler Beanspruchung jedoch aussieht, ist hier nirgendwo nachzulesen. Allerdings hat der Betriebsrat im vorliegenden Fall darauf geachtet, dass der Ausschluss der Nutzung von Informationen zu Kontrollzwecken sich auch auf solche Informationen bezieht, die vom externen Systemanbieter (unrechtmäßigerweise) gewonnen und dem Arbeitgeber zur Verfügung gestellt werden.

Im Vergleich zu der vorausgehenden ausführlichen und in Teilen gut gelungenen Regelung der cloudgestützten Datenverarbeitung ist die nachfolgende Klausel, die sich auf die gleiche Reisekostenabrechnungsanwendung bezieht, wesentlich zu kurz.

> „Mittels Concur erfolgt weder eine maschinelle Leistungs- und Verhaltensprüfung von Mitarbeitern noch ein maschineller Leistungs- und Verhaltensvergleich zwischen Mitarbeitern."
> ➔I Börse/Makler, 090203/76/2014

Sie entspricht dem zuletzt Beschriebenen: Zwar ist es verständlich, dass eine allumfassende Ausschlussklausel alle denkbaren Auswertungen verbieten und damit eine gefühlte Rechtssicherheit herstellen soll – diese existiert jedoch in dieser Form nicht. Warum gerade ein derart kurz gefasster Verwertungsausschluss nicht greift, wird am Ende dieses Kapitels durch die Problembehandlung der Beweisverwertungsverbote ausführlich dargestellt.

Gefährlich sind auch folgende Formulierungen, wenn es um bewusst gewollte Leistungs- und Verhaltenskontrollen geht.

> „Das System darf nicht zum Zweck der Überwachung von Verhalten der Mitarbeiterinnen und Mitarbeiter eingesetzt werden. Eine Erhebung der Daten zum Zwecke der Verhaltenskontrolle benötigt die Zustimmung des Betriebsrates. Aus dem System erhobene Infor-

> mationen können im Zusammenhang mit den Zielvereinbarungen verwendet werden."
>
> ➔ Mess-, Steuer- und Regelungstechnik, 090203/60/2013

Zwar bleibt es dem Arbeitgeber grundsätzlich unbenommen, die Leistung und auch das Verhalten der Arbeitnehmer in bestimmten Bereichen zu prüfen. Er kann und muss teilweise die Arbeitsleitung der Beschäftigten beurteilen und darf dies auch. Die pauschale Erlaubnis „Aus dem System erhobene Informationen können im Zusammenhang mit den Zielvereinbarungen verwendet werden" erlaubt dem Arbeitgeber jedoch jedwede mögliche Auswertung in Zusammenhang mit den Zielvereinbarungen. Letztere können sehr weitreichend und für jeden einzelnen Arbeitnehmer sehr unterschiedlich sein. Nicht nur dem Arbeitgeber, sondern auch dem Cloud-Anbieter eröffnet dies enorme Spielräume bei der Erfassung und Auswertung von detaillierten Beschäftigtendaten.

Bezogen auf zwei weitere Cloud-Anwendungen, die dem After-Sales-Bereich und dem Qualitätsmanagement zuzuordnen sind, gelten die gleichen Grundsätze: Für derart umfangreiche Möglichkeiten, Beschäftigte über Daten aus einem cloudbasierten System bewerten zu können, greifen die in der Vereinbarung manifestierten Regelungen viel zu kurz.

> „Die oben genannten Tools werden ausschließlich zu den vorstehenden Zwecken eingesetzt. Die dabei anfallenden personenbezogenen Daten werden nicht für personelle Maßnahmen für Personen aus den Bearbeitungsteams im arbeitsrechtlichen Sinn erhoben oder genutzt."
>
> ➔ Anonym, 090203/71/2013

Insbesondere weil die in Bezug genommenen „Zwecke" (vgl. Kap. 2.2.2) eben doch gerade solche enthalten, die durchaus auf arbeitsrechtliche Maßnahmen durchschlagen könnten, wie z. B. die Kundenzufriedenheitsbewertung oder die Einhaltung der Service- und Supportverträge mit den Kunden, sind diese Formulierungen zumindest zweideutig. Es bliebe abzuwarten, ob eine solche Formulierung tatsächlich Stand hielte in einem individualarbeitsrechtlichen Prozess gegen einen Kundendienstmitarbeiter, der sich darauf berufen möchte, dass Auswertungen aus diesem System nicht zur Beurteilung einer arbeitsrechtlichen Maßnahme gegen ihn angeführt werden dürfen.

Das Problem der in Betriebsvereinbarungen normierten Leistungs- und Verhaltenskontrollen ist folgendes: Beweiserhebungs- und Verwertungsverbote wurden in letzter Zeit durch die obersten Gerichte des Öfteren diskutiert. Das Bundesarbeitsgericht (BAG) hat sich zwar zur Frage der Beweisverwertung geäußert – jedoch nur betreffs solcher Beweise, die a) unter Missachtung eines Grundrechts (insbesondere des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) oder b) unter Missachtung oder Verletzung der Mitbestimmungsrechte des Betriebsrats erhoben wurden. Hier unterliegt die Beweisverwertung der Verhältnismäßigkeitsprüfung bei der Abwägung zweier Grundrechte: Auf der einen Seite steht das Grundrecht des Arbeitgebers aus Art. 12 GG, seine gewerbliche Tätigkeit störungsfrei durchführen zu können. Auf der anderen Seite steht das Grundrecht des Arbeitnehmers aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG zur Wahrung seiner Persönlichkeitsrechte. Dies führte unter anderem dazu, dass die Formulierungen innerhalb der Urteile recht unbestimmt und für Betriebsräte schwer in betriebsverfassungsrechtliche Formulierungen umzusetzen waren. Es besteht daher bezogen auf die BAG-Rechtsprechung eine nicht unwesentliche Unsicherheit, ob und welche Beweisverwertungsverbote Stand halten würden und welche nicht.

Ein Urteil des Landesarbeitsgerichtes Berlin-Brandenburg (09.12.2009, 15 Sa 1463/09) ist hier deutlicher und in Bezug auf eine Betriebsvereinbarung auch treffender:

> „Dem steht nicht entgegen, dass nach Ansicht des BAG ein Verstoß gegen Mitbestimmungsrechte des Betriebsrates nicht zur Folge hat, dass die insofern gewonnenen Erkenntnisse im arbeitsgerichtlichen Verfahren nicht verwertet werden dürfen (BAG vom 27.03.2003 – 2 AZR 51/02 – NZA 2003, 1193; vom 13.12.2007 – 2 AZR 537/06 – NZA 2008, 1008). Es kann offen bleiben, ob dieser Ansicht des BAG zu folgen ist. Für das BAG war entscheidend, dass weder das Betriebsverfassungsrecht noch die Zivilprozessordnung bei einem Verstoß gegen Mitbestimmungsrechte als Sanktion vorsehen, dass die hieraus gewonnenen Erkenntnisse nicht verwertet werden dürfen. Vorliegend wird die Unwirksamkeit jedoch nicht auf gesetzliche Normen gestützt, sondern auf die Gesamtbetriebsvereinbarung selbst. Diese enthält eine eindeutige Regelung dahingehend, dass personelle Maßnahmen unter bestimmten Voraussetzungen unwirksam sind. Insofern führt der hier festzustellende Verstoß gegen die Verfahrensregelungen in Ziffer 4.3 der GBV zur Unwirksamkeit

> der hiesigen Kündigung. […] Im Gegensatz zu den gesetzlichen Regelungen ist in der Gesamtbetriebsvereinbarung eine eindeutige Sanktionsnorm enthalten. Eine solche Regelung ist auch zulässig."

Es lässt sich also festhalten: Insbesondere jene Beweisverwertungsverbote, die sich auf Leistungs- und Verhaltenskontrollen beziehen, sollten explizit ausformuliert sein. Sie müssen zudem die Konsequenzen des Verstoßes, z. B. den Ausschluss jeglicher personeller Maßnahmen, konkret benennen.

Die Tatsache, dass es sich im vorliegenden Fall um cloudbasierte Datensammlungen handelt, macht die Frage der Verwertbarkeit noch eklatanter. Denn selbst wenn der Arbeitgeber die Daten gar nicht erhalten würde, die hier zu personellen Maßnahmen geeignet wären, könnte gegebenenfalls ein Gericht den Cloud-Anbieter verpflichten, die Daten, die noch vorgehalten werden, nach § 142 Zivilprozessordnung (ZPO) herauszugeben (vgl. Mielchen 2014).

2.2.9 Rechte des Betriebsrats

Wer mehr wissen möchte
http://www.boeckler.de/cps/rde/xchg/hbs/hs.xsl/4129.htm?bvdoku.theme=166#bvdoku1

Je größer der Beteiligtenkreis ist, der zumindest theoretisch Zugriff auf Mitarbeiterdaten bekommen kann, und je größer insgesamt die Datenmengen sind, die über Mitarbeiter gespeichert und verarbeitet werden können, desto umfassender müssen die Rechte der Betriebsräte ausgestaltet sein, die ihnen vorgelegten Informationen prüfen zu können. Wie bereits erwähnt, sollten sich die Kontrollrechte der Gremien sogar auf Externe ausdehnen, um dem eigentlichen Sinn und Zweck des Betriebsverfassungsrechts und des Beschäftigtendatenschutzes noch entsprechen zu können: nämlich dem Schutz der Mitarbeiterinnen und Mitarbeiter. Seit Beginn der Auslagerung der IT-gestützten Datenverarbeitung durch Unternehmen und heute in zunehmendem Maße verlieren Mitbestimmungsgremien den Überblick über die Stellen, die bei der Datenverarbeitung beteiligt sind. Die Sicherungsmechanismen, die zwischen Betriebsrat und Arbeitgeber funktionierten, wer-

den zunehmend aufgeweicht, weil die Vorschriften des Betriebsverfassungsgesetzes nicht gegenüber Dritten wirken, sondern dem Gremium jeweils nur in seinem Verhältnis zum Arbeitgeber Rechte zugestehen. Die in der Theorie funktionierende „vertrauensvolle Zusammenarbeit" zwischen Unternehmen und Betriebsrat wird heute oftmals deswegen ad absurdum geführt, weil die Entscheider auf Unternehmensseite nicht mehr vor Ort, sondern in geografisch weit entfernten Konzernmüttern über den Einsatz von vermeintlich kostengünstigeren Cloud-Datenverarbeitungen entscheiden – ohne sich der gesetzlichen Rechte der Mitarbeitervertretungen bewusst zu sein. Wenngleich nach rein rechtlichen Gesichtspunkten einem Gremium stets ein deutscher Verantwortlicher gegenüberstehen muss, finden Entscheidungen zur Einführung von Cloud-Lösungen oftmals viele Ebenen „weiter oben" statt. Rein faktisch kann sich ein deutscher Geschäftsführer kaum noch wehren, wenn die Konzernspitze europaweit eine bestimmte Datenverarbeitungssoftware einführen will. Trotzdem stehen den deutschen Betriebsräten hierfür zurzeit nur die üblichen rechtlichen Schritte zur Verfügung: Sie müssen ihre Ansprüche gegenüber „ihrem" Arbeitgeber geltend machen. Hierzu bedarf es hinsichtlich externer, dynamischer Cloud-Datenverarbeitung ausgeklügelter Klauseln, um die Rechte des Gremiums zu wahren. In den vorliegenden Vereinbarungen wurde teilweise versucht, dies zu erreichen. Im Rahmen der offenbar nur eingeschränkt bekannten Fakten über Cloud-Lösungen ist dies auch geschehen. Mitunter scheinen Mitbestimmungsgremien jedoch weitreichende Rechte aufgegeben zu haben – sei es aus Unterschätzung des Risikopotenzials oder aus zeitlicher Überforderung mit dem Thema. Beispielsweise wird darauf verzichtet, bereits in der Testphase seine Mitbestimmungsrechte auszuüben, obwohl hier noch das größte Potenzial an Mitwirkungsmöglichkeiten bestünde.

> „Einer Zustimmung bedarf es nicht für Testläufe, die ausschließlich der Überprüfung von Funktion oder Sinnhaftigkeit einer neuen oder wesentlich geänderten Software zur Spesen- oder Promotionabrechnung dienen."
>
> →| Großhandel (ohne Kfz.), 090503/43/2009

In der gleichen Vereinbarung wird zudem einschränkend darauf verwiesen, dass das Gremium nur „auf Wunsch" Zugriff auf die notwendigen Dokumente erhalten soll.

> „Dem Betriebsrat wird auf Wunsch die vorhandene Dokumentation der eingesetzten Concur-Software in geeigneter Form (z. B. online) zugänglich gemacht."
>
> ➔ Großhandel (ohne Kfz.), 090503/43/2009

Grundsätzlich wurde jedoch versucht, weitreichende Kontrollmöglichkeiten zu beschreiben. Eine Zustimmungsfiktion, wie sie hier implementiert ist, sollte allerdings möglichst vermieden werden. Dass die Zustimmung als erteilt gilt, soweit nicht in der unmittelbar nächsten Sitzung nach der Information durch den Arbeitgeber eine Entscheidung getroffen wurde, ist vermutlich dem Wunsch nach einem reibungslosen Ablauf bei der Implementierung von Updates oder neuen Versionen der cloudgestützten Software geschuldet. Dies geht jedoch zu weit, da überhaupt nicht abgeschätzt werden kann, welche wesentlichen Informationen über neue Module, neue „Fähigkeiten des Systems" oder neue beteiligte Unternehmen in rechtlich unsicheren Staaten bei einer Veränderung des Systems hinzukommen können.

> „Alle Maßnahmen, die mit der Einführung oder wesentlichen Änderung von Concur zusammenhängen, sind dem Betriebsrat rechtzeitig und umfassend bekanntzugeben und mit ihm gemäß § 90 BetrVG zu beraten. Die Unterrichtung ist in allgemein verständlicher Form zu gestalten oder bei technischen Dokumentationen mit entsprechenden Erläuterungen zu versehen. Sie erfolgt in Deutsch.
> Eine wesentliche Änderung […] bedarf der Zustimmung des Betriebsrats, bevor sie produktiv gesetzt wird. Wird [sie] dem Betriebsrat […] zur Zustimmung vorgelegt, wird er spätestens bei der unmittelbar auf den Zustimmungsantrag folgenden Betriebsratssitzung dazu Stellung nehmen und die Zustimmung erteilen oder verweigern, ansonsten gilt die Zustimmung als erteilt.
> Der Betriebsrat ist berechtigt, jederzeit die Einhaltung dieser Betriebsvereinbarung zu überprüfen. Ihm wird die uneingeschränkte Einsichtnahme in Concur einschließlich aller Protokolle (z. B. die audit logs) und Systeminformationen, Laufwerke und Berichte gewährt, wobei er durch die zuständigen Personen unterstützt wird. Dabei wird der Betriebsrat darauf achten, dass durch eine solche Einsichtnahme der reibungslose Arbeitsablauf der entsprechenden Abteilungen nicht oder nicht mehr als unbedingt erforderlich beeinträchtigt wird."
>
> ➔ Großhandel (ohne Kfz.), 090503/43/2009

Besonders sinnvoll ist es, die entsprechenden Systemverantwortlichen dem Betriebsrat gegenüber zur Auskunft zu verpflichten und gleichzeitig ein Benachteiligungsverbot offen zu kommunizieren.

> „Alle Personen, die mit Concur arbeiten, sind gegenüber dem Betriebsrat im Rahmen ihrer Aufgaben auskunftsberechtigt, soweit dies für Kontrollzwecke des Betriebsrats erforderlich ist. Diese Auskunft darf für diese Personen zu keiner Benachteiligung führen."
> ➔I Großhandel (ohne Kfz.), 090503/43/2009

Zwar ist es gesetzlich verankert, dass ein Gremium stets nach § 80 Abs. 3 BetrVG einen Sachverständigen hinzuziehen darf, wenn dies aufgrund fehlenden Sachverstandes im Gremium erforderlich ist; dennoch macht es einen großen Unterschied, wenn der Betriebsrat in der Vereinbarung die Prüfpflichten der Erforderlichkeit verkürzt. Teilweise ist es sehr zeitintensiv, im Streitfall mit dem Arbeitgeber die Erforderlichkeit feststellen zu lassen. Nach der folgenden Formulierung unterliegt das Gremium nur noch einer eingeschränkten Prüfpflicht, ob der Sachverständige tatsächlich „zur Kontrolle der Einhaltung und zur Umsetzung der Betriebsvereinbarung" beauftragt wird. Dies ist im Ergebnis eine Zeitersparnis, die die Zeitspanne der Einführung einer solchen Anwendung deutlich verkürzen kann. Trotzdem dürfte sie nicht jedem Arbeitgeber gegenüber durchzusetzen sein.

> „Der Betriebsrat kann zur Kontrolle der Einhaltung und zur Umsetzung der Betriebsvereinbarung einen externen Sachverständigen seiner Wahl beauftragen."
> ➔I Großhandel (ohne Kfz.), 090503/43/2009

Sinnvollerweise wird auf die Kontrollmöglichkeiten des Betriebsrats bei der Erstellung oder Implementierung neuer Auswertungsmöglichkeiten detailliert eingegangen. Da es sich hierbei wie bei jeder wesentlichen Systemveränderung im Grunde um ein neu auszuübendes Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG handelt, sollte dieses Recht allerdings nicht auf ein bloßes Beratungsrecht verkürzt werden. Nachstehend wurde dies gelöst, indem bei Unstimmigkeiten die Anrufung der Einigungsstelle gemäß § 76 Abs. 5 BetrVG direkt in die Betriebsvereinbarung aufgenommen wurde. Die Beschreibung der Rechte zur Einsichtnahme und der Informationspflichten der Arbeitgeberseite wiederholen hingegen lediglich die gesetzliche Lage.

> „Alle neuen Reports sind vor der Einführung dem Betriebsrat vorzustellen, damit eine Konformität innerhalb der Betriebsvereinbarung geprüft werden kann. […]
> Der Betriebsrat hat das Recht, alle vorhandenen Unterlagen über das System einzusehen und sich erläutern zu lassen.
> Der Betriebsrat wird über alle geplanten Änderungen, insbesondere Erweiterungen, vor deren Einführung informiert. Bei dieser Gelegenheit beraten beide Seiten, ob die Bestimmungen dieser Vereinbarung eingehalten sind.
> Macht der Betriebsrat geltend, dass sich durch die geplanten oder auch durch zwischenzeitliche Änderungen des Systems oder des Umgangs mit dem System neue, nicht gesetzeskonforme Probleme bezüglich des Persönlichkeitsschutzes nach dem Bundesdatenschutzgesetz der Mitarbeiterinnen und Mitarbeiter ergeben, so hat er das Recht, eine zu dieser Vereinbarung ergänzende Regelung zu verlangen. Über diese wird mit dem Ziel einer einvernehmlichen Lösung verhandelt. Kommt in den Fällen, in denen diese Vereinbarung das Einvernehmen beider Seiten vorsieht, eine Einigung nicht zu Stande, so entscheidet eine gemäß § 76 Abs. 5 BetrVG zu bildende Einigungsstelle."
> ➔ Börse/Makler, 090203/60/2014

Auch in der folgenden Textpassage einer Vereinbarung verkürzt der Betriebsrat seine Rechte. Statt nach § 80 Abs. 2 BetrVG die gesetzlich vorgeschriebene Informationspflicht der Arbeitgeberseite auszuschöpfen, begnügt er sich mit einem Antragsrecht. Dies ist unverständlich, denn die Erfahrung zeigt: Sogar trotz Bestehen der gesetzlichen Verpflichtung nach § 80 Abs. 2 BetrVG („Zur Durchführung seiner Aufgaben nach diesem Gesetz ist der Betriebsrat rechtzeitig und umfassend vom Arbeitgeber zu unterrichten") muss der Betriebsrat oft mehrfach und zeitintensiv die entsprechende Unterrichtung anmahnen. Gleiches gilt für das Recht, sich anlassbezogene Protokolle aushändigen zu lassen. Es ist davon auszugehen, dass hiermit die Vorlage von Protokollen im Fall von Beanstandungen beim Einsatz des Systems gemeint ist („anlassbezogen"). Wesentlich besser wäre es hingegen, anlassunabhängige Kontrollen in der Betriebsvereinbarung festzulegen.

> „Auf Antrag hat der Betriebsrat das Recht der Einsichtnahme in die Reportinglisten. Der Antrag ist binnen 2 Wochen zu bearbeiten.

> […]
> Jede Änderung des Berechtigungskonzeptes bedarf der ausdrücklichen Einwilligung des BR. […]
> Der Betriebsrat hat einen Anspruch, zur Überprüfung der Einhaltung dieser Betriebsvereinbarung den Beauftragten für den Datenschutz zu befragen und anlassbezogen Zugriffs- und Auswertungsprotokolle einzusehen und sich ggfs. aushändigen zu lassen."
> ➔ Anonym, 090203/71/2013

2.2.10 Veränderung von Geschäftsprozessen, Rationalisierungsgefahr

Die Einführung von cloudbasierten Anwendungen in Unternehmen wird zumeist mit dem erheblichen Potenzial zu Einsparungen begründet. Es müssten künftig wesentlich weniger eigene IT-Ressourcen vorgehalten werden, weil diese dynamisch hinzugebucht werden könnten, falls zeitweilige Auslastungen im Betrieb dies erfordern sollten. Das Vorhalten einer erheblichen Anzahl von Lizenzen würde wegfallen und auch die Betreuung der Systeme würde weniger personelle Kapazitäten beanspruchen. Gerade aufgrund der von Unternehmensseite offen kommunizierten Hintergründe für den „Schritt in die Cloud" ist es erstaunlich, dass die vorliegenden Vereinbarungen keine Aussagen dazu treffen, wie mit dem Risiko von kurz- oder mittelfristigem Personalabbau umzugehen ist. Es finden sich auch keine Klauseln zur Arbeitsplatzsicherung. Möglicherweise realisiert sich aber gerade hier die Gefahr, auf die bereits bei der Beschreibung des Regelungsgegenstandes (Kap. 2.2.1) hingewiesen wurde: Indem in keiner der Vereinbarungen die mittlerweile bzw. künftig genutzten Clouds als solche thematisiert werden, werden die Risiken überhaupt wahrgenommen.

In keiner ausgewerteten Vereinbarung wird zudem darauf eingegangen, dass durch die beständig wachsende, für die Zukunft unendlich erscheinende Verfügbarkeit von IT-Ressourcen der Weg geebnet wird in ein „Verfügbarkeitsverlangen" des Arbeitgebers in Bezug auf seine Arbeitnehmer. Früher stießen Unternehmen an Grenzen: die begrenzt verfügbaren Rechnerkapazitäten, die mangelhaften Möglichkeiten der länderübergreifenden Zusammenarbeit von Arbeitnehmern aufgrund der unterschiedlichen Zeitzonen oder auch „nur" die Einschränkungen, die durch örtlich gebundene und damit dem deutschen Arbeitsrecht unterliegende Beschäftigte gegeben waren. Sind jedoch das Wissen eines Unternehmens, sein Know-how, seine struktu-

rellen Gegebenheiten und seine Arbeitsprozesse immer und überall mobil und ohne Kapazitätsengpässe verfügbar, lösen sich die Grenzen von Unternehmen auf. Im positiven Sinne mag dies die Flexibilität von Arbeit erhöhen und die Lebensmodelle von Arbeitnehmern unterstützen, die auf örtliche und zeitliche Ungebundenheit angewiesen sind oder diese einfach bevorzugen. Im negativen Sinne stoßen diese sich auflösenden Grenzen an die weiterhin bestehenden Grenzen der „Ressource Mensch".

Der Schritt vom Cloud-Working in Unternehmen hin zu einem weltweiten, anonymen „Crowd-Working in der Cloud" ist nicht mehr allzu groß. Warum sollte sich ein Unternehmer künftig mit Urlaubsansprüchen oder Arbeitszeitfragen deutscher Arbeitnehmer auseinandersetzen, wenn er die entsprechenden Aufgaben auch genauso gut in einem anderen Teil der Welt, in Echtzeit und innerhalb der gleichen Infrastruktur bearbeiten lassen kann wie bereits jetzt: in der Cloud? Ein animierter Kurzfilm von ver.di macht dieses Dilemma auf spielerische Art deutlich: „Claus der Cloudworker"[9] zeigt, welche Auswirkungen es haben kann, wenn geistige Arbeit mit allen internationalen verfügbaren „personellen Ressourcen" konkurrieren muss. Ein Crowd-Working im besonderen Sinne: Menschen, die sich nie kennenlernen, arbeiten zusammen, stellen ihre Teilergebnisse online zur Verfügung in den Datenwolken dieser Welt und warten, ob sie in ihrem Teilbereich die besten Ergebnisse abgeliefert haben. Ist dies nicht so, gehen sie leer aus. Schutzmechanismen mühsam entwickelter und gewachsener gesetzlicher Rahmenbedingungen laufen ins Leere[10].

Unter dieser Prämisse müssen künftige Vereinbarungen, die sich auf cloudgestützte Anwendungen beziehen, Regelungen beinhalten, die den Mitbestimmungsgremien weitgehend ihre Rechte sichern und damit den Schutz der Beschäftigten aufrechterhalten. Hier besteht zurzeit noch eine große Lücke und erheblicher Handlungs- und Nachbesserungsbedarf.

2.3 Problematik der cloudfähigen Software

Wie bereits in Kapitel 2.2 mehrfach erwähnt, haben alle vorliegenden Betriebsvereinbarungen eines gemeinsam: Sie benennen nie ausdrücklich die

9 Vgl. Stuckmann u. a. (2012), www.verdi.de/themen/arbeit/++co++fd9e2f52-82fe-11e1-5004-0019b9e321e1 [22.2.2016].

10 Ein Beratungsangebot der Gewerkschaft ver.di für Cloud-Worker findet sich seit diesem Jahr unter www.cloudworker-beratung.de.

Tatsache, dass es sich bei dem Regelungsgegenstand um eine cloudgestützte Datenverarbeitung handelt. Meist kann nur aufgrund der Bezeichnung der Softwareanwendungen und weiterer Hintergrundrecherchen festgestellt werden, dass die Beschäftigtendaten jeweils in ein Speicher- und Verarbeitungsmedium gelangt sind, das dem Unternehmen entweder die Software oder gleich die gesamte Verarbeitungsumgebung als Dienst zur Verfügung stellt. Örtliche Eingrenzungen lassen sich so nur noch schwer feststellen, Zugriffsberechtigte nur noch schwer benennen und die Durchsetzung von Rechten der Beschäftigten nur noch schwer bewerkstelligen.

Eine weitere Besonderheit bei der Auswertung der vorliegenden Vereinbarungen war folgende Feststellung: Trotz Zuhilfenahme weiterer Informationsquellen lässt sich bei manchen Vereinbarungen nicht definieren, ob es sich um eine cloudgestützte Softwareanwendung handelt oder nicht. Die Gründe sind einfach: Einige Dienste sind im Laufe der Zeit quasi „in die Cloud gewandert" – ohne genaue Benennung, um welche Version der Anwendung es sich handelt, kann nicht festgestellt werden, ob sie „noch" vor Ort auf einem eigenen oder auf einem in Deutschland beheimateten Server eines IT-Dienstleisters läuft oder „schon" in eine internationale Cloud ausgelagert wurde. Es steht zu vermuten, dass gegebenenfalls zunächst das eine und dann unbemerkt das andere stattgefunden hat.

Ein anderer Grund ist beispielsweise, dass die Bezeichnungen in der Vereinbarung derart unspezifisch gewählt wurden, dass nicht erkennbar ist, ob es sich um eine cloudgestützte Datenverarbeitung handelt oder nicht. Wenn beispielsweise keine einheitliche Definition des Begriffs „Unified Communication" existiert, könnte eine derart bezeichnete Anwendung in einer Datenwolke zur Verfügung gestellt werden; es könnte sich jedoch auch um einen Titel handeln, der verschiedene integrierte Kommunikationsdienste bezeichnet, die weiterhin auf unternehmenseigenen Rechnern zur Verfügung gestellt werden. Das bedeutet: Beim Abschluss einer Betriebsvereinbarung muss unbedingt darauf geachtet werden, was für ein System überhaupt geregelt wird. Um den Blick dafür zu schärfen, werden im Folgenden einige Beispiele aufgezeigt.

Ein klassisches Exempel hierfür ist die Kollaborationsplattform SharePoint von Microsoft. Diese Anwendungen haben eine lange Geschichte und unterscheiden sich in ihrer Bezeichnung und – was viel wichtiger ist – in ihrer dahinterstehenden Architektur seit ihrem Beginn als SharePoint Portal Server 2001 bis hin zur heutigen Anwendung(splattform) SharePoint 2013 extrem. Regelt nun eine Betriebsvereinbarung aus dem Jahr 2010 die Einführung der Software Windows SharePoint Services, stellt sich die Frage: Was ge-

nau ist damit gemeint? Handelt es sich dabei „nur“ um ein Unternehmensportal, das über eine Web-Oberfläche einen zentralen, personalisierten Zugriff auf Inhalte des Intranets bietet? Oder ist das Unternehmen mittlerweile im Cloud-Zeitalter angekommen und nutzt SharePoint online? Beides wäre nach der Bezeichnung in der Vereinbarung möglich. Den Formulierungen ist jedenfalls nichts zu entnehmen, was die Frage beantwortet – und es handelt sich hierbei um den gesamten Vereinbarungstext!

> „Anwendung der Software Microsoft Windows SharePoint Services
> – Der Gesamtbetriebsrat wird über die eingesetzten Module und deren Verwendungszweck informiert.
> – Personenbezogene Auswertungen und Auswertungen, die Rückschlüsse auf die Leistung und das Verhalten von Mitarbeitern zulassen, werden nicht durchgeführt.
> – Der Gesamtbetriebsrat erhält Informationen welche Daten im Einzelnen eingepflegt werden. Diese Daten werden nicht für personalrechtliche Maßnahmen verwendet.
> – Mit dieser Software werden keine grundlegend neuen Arbeitsmethoden im Sinne des § 111 BetrVG beabsichtigt bzw. eingeführt.
>
> Der Gesamtbetriebsrat stimmt dem Betrieb der MS SharePoint Services zu.“
>
> ➔ Gesundheit und Soziales, 090201/449/2010

Das erwähnte Beispiel einer Vereinbarung zur Einführung einer Unified-Communication-Pilotanwendung bietet ebenfalls keine weitergehenden Informationen, die echte Klarheit schaffen. Zwar wird versteckt (in den Anlagen) der Produktname genannt und es ist aus der Bezeichnung Lync Server zu schließen, dass es sich vermutlich nicht um eine cloudbasierte Lösung handelt. Eine Betriebsvereinbarung sollte jedoch zu dieser Frage konkret Stellung nehmen und keinen Spielraum für Vermutungen lassen.

> „Definition Unified Communication (nachfolgend UC-Pilot genannt): Integration der verschiedenen Kommunikationsdienste und -funktionen unter einer einheitlichen, standardisierten und einfach zu bedienenden Oberfläche.
> Der UC-Pilot soll die Vorteile einer Unified Communication Lösung für [die Firma] aufzeigen und belegen. Vor allem sollen die für

[die Firma] neuen Funktionen wie IMS (Instant Messaging/Chat) und Präsenzinformation und deren Auswirkung getestet werden.
Die pilotiert UC-Infrastruktur ist in der Anlage 1 aufgeführt und wird dort gepflegt.
Eine Beschreibung des Pilotumfanges ist in Anlage 2 hinterlegt. […]
Anlage 1 […]
a) 1 x Unified Communication Server ‚LYNC' […]
Anlage 2 […]
– Pilotumfang/Funktionen: IMS/Chat, Anzeige der Präsenzinformationen, VOIP, Telefon-Konferenzen, WEB-Konferenzen […]."

→| Fahrzeughersteller von Kraftwagenteilen, 090300/216/2010

3 MITBESTIMMUNG: RECHTE UND VERFAHREN

Zwar gewinnen die Mitbestimmungsrechte des Betriebsrats gerade bei internationaler Datenverarbeitung von Beschäftigtendaten zunehmend an Bedeutung; dennoch enthalten die vorliegenden Vereinbarungen kaum mehr als die üblichen Formulierungen zur Ausgestaltung derselben bzw. als man bei Regelungen zum Einsatz von standortbezogenen IT-Anwendungen erwarten würde. Selbstverständlich ist bereits die Tatsache, dass Betriebsvereinbarungen zu cloudbasierter Software abgeschlossen wurden – wenngleich dies nicht explizit erwähnt wird – Ausdruck für das grundlegend geltende Recht, gemäß § 87 Abs. 1 Nr. 6 BetrVG mitzubestimmen bei der Einführung und Anwendung einer Technologie, die zur Überwachung der Mitarbeiter geeignet ist. Hierbei kommt es nicht auf den Willen des Arbeitgebers an, eine solche Überwachung zu planen. Vielmehr genügt es, dass die Technologie dem Arbeitgeber grundsätzlich die Möglichkeit dazu gäbe. Bei der Einführung von IT-gestützten Verfahren ist heute selten ein Fall denkbar, bei dem diese Möglichkeit nicht bestünde. Allein dann, wenn überhaupt keine personenbezogenen Daten im System verfügbar wären oder zumindest in keiner Weise verknüpft werden könnten, käme dieser Ausnahmefall in Betracht. Gleiches gilt dann auch für den Einsatz von cloudbasierter Software.

Die einzige Formulierung, die sich konkret mit dem Thema beschäftigt, findet sich in einer Vereinbarung aus dem Jahr 2013 zur Vertriebs- und Kundenmanagementsoftware Salesforce. Nicht nachvollziehbar ist dabei, dass zwar in der Vereinbarung an anderer Stelle genau auf das Verbot von Überwachungsmaßnahmen eingegangen wird, jedoch hinsichtlich des Themas Personenbezogene Daten im System Folgendes geregelt ist.

> „Das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG insbesondere in Bezug auf die elektronische Datenerfassung und die Nutzung des Systems Salesforce.com bleiben vollständig unberührt."
> ➔ Mess-, Steuer- und Regelungstechnik, 090203/60/2013

Ob das Gremium weitergehende Regelungen in naher Zukunft schaffen wollte, kann hier nicht beurteilt werden. Fakt ist jedoch, dass die Ausgestaltung dieses Mitbestimmungsrechts wesentlich mehr Möglichkeiten beinhaltet, als hier ausgeschöpft wurden. Im Rahmen der Ausgestaltung des zwingenden Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 ist zunächst daran zu

denken, dass ein weiteres Recht den Gremien erst zu der Möglichkeit verhilft, zu beurteilen, welche Risiken durch eine Vereinbarung zu minimieren oder zu unterbinden sind. Nach § 80 Abs. 2 BetrVG kann der Betriebsrat verlangen, vor Einführung solcher neuen Anwendungen frühzeitig und umfassend unterrichtet zu werden. Bei einer cloudgestützten Software müssen diese Informationsrechte sehr detailliert genutzt werden, um alle entstehenden Gefahren beurteilen zu können. Wesentlich hierbei sind Auskünfte über die einzusetzende Software genauso wie über die dahinterstehende Cloud-Lösung, die der Arbeitgeber zu nutzen plant. Hilfreich kann hier zunächst ein Benutzerhandbuch sein, das auch in Zeiten onlinegestützter Verfahren oftmals noch zur Verfügung steht. Gerade Handreichungen für die unternehmensinterne IT-Abteilung darüber, wie das System funktioniert und wie es in die bestehenden Systeme zu integrieren ist, können dem Gremium ausführliche Hinweise dahingehend liefern, welche Daten der Beschäftigten im System gespeichert und verarbeitet werden und welche Auswertungen möglich sind. Es finden sich Hinweise zu Schnittstellen zu anderen Anwendungen ebenso wie Angaben über Speicherfristen, Wege der Datenflüsse, unterschiedliche Benutzerrollen und vieles mehr. Oftmals sind diese Handbücher auf dem Web-Portal des Anbieters verfügbar.

Allerdings gibt es bezüglich dieser Informationsquellen ein insbesondere bei internationalen Konzernen immer virulenter werdendes Problem: Die Entscheider-Ebene, die die Einführung der entsprechenden cloudbasierten Software beschließt, ist oftmals nicht mehr in europäischen oder deutschen Standorten des Arbeitgebers angesiedelt. Häufig wird die Einführung einer cloudgestützten Software auf Konzernebene entschieden, um im gesamten Unternehmen die gleichen Arbeitsvoraussetzungen in bestimmten Abteilungen oder Fachbereichen zu schaffen und dadurch letztlich die Effizienz zu steigern. Damit sollen nicht nur Schnittstellenprobleme abgeschafft werden; insbesondere gilt es, die Nutzung solcher Anwendungen seitens Mitarbeiter sowie deren Schulung effizienter zu gestalten. Hierbei wird in geografisch weit entfernten Konzernzentralen jedoch oft übersehen, dass auch die in anderen Ländern beheimateten Unternehmensteile konkrete Informationen über die Veränderungen benötigen. Nicht selten ist der in Deutschland befindliche Arbeitgeber nur spärlich darüber informiert, was genau von der Konzernspitze geplant ist. Die Praxis zeigt, dass Führungskräften hierzulande zunächst oft nur der Produktname und ein zwingendes Einführungs- bzw. Releasedatum mitgeteilt wird. Dies genügt jedoch für die als Arbeitgebervertreter fungierenden Akteure wie Geschäftsführer oder Personalleiter nicht, um die Gremien vor Ort frühzeitig und umfassend zu informieren.

Die Folge ist ein Informationsdefizit seitens des deutschen Arbeitgebers sowie seitens der Mitarbeitervertretung, das in einem Ping-Pong-Spiel aus Fragen und nicht verfügbaren Antworten kulminiert und die Hilflosigkeit der Betroffenen zur Schau stellt. Teilweise werden deutschen Unternehmensleitungen nur Eckpunkte von solchen Neuerung mitgeteilt, die der internationale Verantwortliche als wissenswert für die in den einzelnen Ländern arbeitenden Führungskräfte erachtet. Dabei wird naturgemäß mehr Wert gelegt auf die praktischen Fragen zur Implementierung des Systems in die vorhandene Infrastruktur der Konzernteile, als daran zu denken, dass gesetzliche Vorschriften vor Ort geprüft werden müssen. Der deutsche Arbeitgeber ist demnach oft de facto gar nicht in der Lage, das System genau zu bezeichnen oder weitergehende Auskünfte über die erfassten Daten zu geben. Dies kann eine deutsche Mitarbeitervertretung jedoch nicht als unabänderlich hinnehmen – würden doch so ihre Mitbestimmungsrechte ad absurdum geführt.

In solchen Fällen kann mit dem Instrument der zwingenden Mitbestimmung aus § 87 Abs. 1 Nr. 6 BetrVG auf die Arbeitgeberseite eingewirkt werden, dass diese wiederum die Konzernverantwortlichen in anderen Teilen der Welt darüber informiert, welche Mitteilungspflichten in Deutschland bestehen. Meist werden notwendige Informationen vermutlich schnell nachgeliefert werden, wenn der auf Konzernebene verantwortliche IT- oder HR-Manager (Personalleiter) erkennt: In Deutschland kann die Einführung des Systems so lange nicht vorangetrieben werden, bis die entsprechenden Informationen geflossen sind. Hierfür muss das Gremium jedoch seine Rechte deutlich einfordern und gleichzeitig gewillt sein, gegebenenfalls alle Instrumente zu nutzen, um sie durchzusetzen.

Ein weiteres Problem, dass beim Einsatz von cloudgestützten Verfahren auf die Interessenvertretungen zukommt, sind die bereits in Kapitel 1 angesprochenen Verträge, die ein Unternehmen abzuschließen hat, um datenschutzrechtlich den Weg der Daten international abzusichern. Um ein angemessenes Datenschutzniveau zu erreichen bei Transfers von Beschäftigtendaten in Clouds, die nicht in Europa beheimatet sind, müssen sichernde Verträge abgeschlossen werden: zwischen den einzelnen beteiligten Unternehmensteilen und dem oder den externen Anbieter/n der cloudgestützten Softwarelösung (vgl. Kap. 6.2). Hierbei ist jedoch selbstverständlich der deutsche Arbeitgeber Vertragspartner und nicht das Gremium selbst, dass als Teil des deutschen Unternehmens keine eigene Rechtspersönlichkeit besitzt. Die Problemlage, die sich auftut, ist die Tatsache, dass in vielen Betriebsvereinbarungen zur Einführung einer solchen Cloud-Anwendung hierauf nicht ausreichend Rücksicht genommen wird. Viele Vereinbarungen – dies zeigt die

vorliegende Auswertung – nehmen gar nicht darauf Bezug. Die Konsequenz: Das Gremium hat kaum eine Durchsetzungsmöglichkeit dahingehend, den Arbeitgeber zu veranlassen, diese für ihn zwingenden Regelungen einzuhalten. Zwar hat die Mitarbeitervertretung gemäß § 80 Abs. 1 Nr. 1 BetrVG das Recht und die Pflicht, den Arbeitgeber zur Einhaltung aller für die Belegschaft schützenden Normen anzuhalten. Dies ist jedoch, sobald eine entsprechende Betriebsvereinbarung erst einmal unterzeichnet ist, weder im Wege eines Beschlussverfahrens noch durch eine Einigungsstelle zu erreichen. Das BetrVG sieht hier lediglich den nicht justiziablen Weg der vertrauensvollen Zusammenarbeit zwischen Betriebsrat und Arbeitgeber vor.

Anders ist die Lage, wenn das Gremium den Abschluss der Verträge zwischen Arbeitgeber und externem Cloud-Anbieter als zwingende Voraussetzung mit in die Betriebsvereinbarung übernommen hatte – am besten inklusive einer Frist, bis zu der die Unterzeichnung der Legitimationsverträge zum Datenaustausch erfolgt sein soll. Hält der Arbeitgeber insoweit die Bestimmungen der Betriebsvereinbarung nicht ein, stellt dies einen Verstoß gegen § 77 Abs. 1 Satz 1 BetrVG dar und der Betriebsrat kann gerichtlich die Durchführung der Vereinbarung verlangen. Alternativ kann das Wirksamwerden der Betriebsvereinbarung direkt vom Abschluss der genannten Verträge abhängig gemacht werden. Kommen die entsprechenden Verträge dann nicht zustande, ist die Betriebsvereinbarung unwirksam, das zwingende Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG kann weiterhin ausgeübt werden und die Verhandlungen müssten dann als gescheitert erklärt werden. Dann stünde der Weg in die Einigungsstelle nach § 76 Abs. 5 BetrVG offen.

Dem Betriebsrat stehen aber auch noch andere Rechte aus dem BetrVG zu. Zunächst ist an die Rechte aus § 87 Abs. 1 Nr. 7 BetrVG zu denken. Auch Software-Ergonomie kann einen Aspekt des Gesundheitsschutzes darstellen, der bei cloudgestützter Datenverarbeitung immer überprüft werden sollte. Zudem können Rechte nach § 87 Abs. 1 Nr. 1 BetrVG (Ordnung im Betrieb) oder § 87 Abs. 1 Nr. 3 BetrVG (Beginn und Ende der Arbeitszeit) einschlägig sein. Dies hängt jedoch wesentlich von der Art der Anwendung ab. Zudem muss geprüft werden, ob die Einführung einer cloudbasierten Software eine Betriebsänderung darstellt (vgl. Wedde 2014). Sind die Voraussetzungen des § 111 BetrVG erfüllt, kann hier über den Abschluss eines Interessenausgleichs oder eines Sozialplans nachgedacht werden. Und der Betriebsrat sollte auch stets an seine Rechte auf Qualifizierung gemäß § 37 Abs. 6 BetrVG denken. Gerade für die Beurteilung vollkommen neuer, teilweise technologisch schwer zu verstehender Verfahren müssen dem Gremium Kenntnisse vermittelt werden, damit es seine Rechte überhaupt ausüben kann.

4 OFFENE PROBLEME

4.1 EuGH-Urteil zum Safe-Harbor-Abkommen vom 6. Oktober 2015

Eines der drängendsten offenen Probleme stellt zurzeit das in Kapitel 1 dargestellte Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 dar. Die Folgen dieser neuen Rechtsprechung sind heute noch nicht vollständig absehbar.

Der Europäische Gerichtshof hat mit diesem Urteil zwar explizit das Safe-Harbor-Abkommen angegriffen und die weiteren Möglichkeiten, die einen internationalen Transfer von Beschäftigtendaten rechtfertigen können, nicht ausdrücklich genannt und damit auch nicht ausdrücklich in Frage gestellt. Die Formulierungen der Urteilsbegründung können jedoch auch derart gelesen werden, dass alle weiteren Rechtfertigungsmöglichkeiten für den internationalen Datenverkehr (EU-Standardvertragsklauseln etc.) durch die Entscheidung des Gerichts ebenso obsolet geworden sind. Denn das Argument, das gegen das Safe-Harbor-Abkommen zu Recht ins Feld geführt wurde – nämlich die Tatsache, dass trotz des Abkommens US-amerikanische Behörden (Geheimdienste) jederzeit die Herausgabe von persönlichen Daten von Unternehmen erzwingen können – greift auch bei der Anwendung der EU-Standardvertragsklauseln oder der konzerninternen Corporate Binding Rules. Auch diese stellen keinen abschließenden Schutz gegen Übergriffe auf europäische Beschäftigtendaten dar. Es stellt sich nur zurzeit die Frage, wie mit dieser Tatsache umgegangen werden muss.

Es kann keine Option sein, ab sofort jeden Datenverkehr aus Europa in die USA oder in andere Länder ohne angemessenes Datenschutzniveau zu unterbinden. Dies würde binnen kürzester Zeit für viele deutsche Arbeitgeber ein völliges Chaos im Betriebsablauf erzeugen, was sicherlich weitreichende Auswirkungen hätte. Ebenso würden vermutlich erhebliche Einbußen bei den internationalen Auftragsdatenverarbeitern entstehen, deren europäischen Kunden plötzlich den Datenverkehr für einen unabsehbaren Zeitraum einstellen würden.

Für seine rigide Haltung, wenn es um die Einhaltung europäischer oder deutscher Datenschutzgesetze geht, ist seit langem das Unabhängige Landeszentrum für Datenschutz Schleswig-Holsteinische (ULD) bekannt. Dieses

hatte binnen kürzester Zeit eine Stellungnahme[11] zum Urteil des EuGH veröffentlicht, in der sie bekannt gab, dass nach ihrer Rechtsansicht nicht nur das Safe-Harbor-Abkommen hinfällig sei, sondern gleichsam sowohl die Einwilligungslösungen als auch die EU-Standardvertragsklauseln keinen rechtfertigenden Schutz mehr gewährleisten würden. Die wesentliche Aussage des ULD hinsichtlich der EU-Standardvertragsklauseln lautet: „In konsequenter Anwendung der Vorgaben des EuGH in seinem Urteil ist eine Datenübermittlung auf Basis von Standardvertragsklauseln nicht mehr zulässig." Zusammengefasst ist die Begründung hierfür: Laut Klausel 5b) der Standardvertragsklauseln müsse der im „unischeren" Drittstaat agierende Datenimporteur garantieren, dass „er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen […]." Dies eben könne der Datenimporteur jedoch nicht garantieren, da er beispielsweise in den USA dem sogenannten Patriot Act unterliege, der den US-Behörden (Geheimdienst) weitreichende Zugriffsmöglichkeiten auf Daten gebe – was wiederum gegen die EU-Standardvertragsklauseln verstieße.

Ob diese Begründung stichhaltig ist, müsste in einer ausführlicheren Stellungnahme geprüft werden, denn die EU-Standardvertragsklauseln sehen auch weitreichende Ausnahmen vor. In einer Fußnote ist zu lesen, dass unter die oben genannten Gesetze nicht solche fallen, die – zusammengefasst – den demokratischen Grundsätzen von Rechtsstaat und Sicherheit dienen:

„Zwingende Erfordernisse des für den Datenimporteur geltenden innerstaatlichen Rechts, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft für den Schutz eines der in Artikel 13 Absatz 1 der Richtlinie 95/46/EG aufgelisteten Interessen erforderlich ist, widersprechen nicht den Standardvertragsklauseln, wenn sie zur Gewährleistung der Sicherheit des Staates, der Landesverteidigung, der öffentlichen Sicherheit, der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, eines wichtigen wirtschaftlichen oder finanziellen Interesses eines Mitgliedstaats, des Schutzes der betroffenen Person und der Rechte und Freiheiten anderer Personen erforderlich sind. Beispiele für zwingende Erfordernisse, die nicht über das hinausgehen, was in einer demokratischen Gesellschaft erforderlich

11 Positionspapier vom 14.10.2015 des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf [22.2.2016].

ist, sind international anerkannte Sanktionen, Erfordernisse der Steuerberichterstattung oder Anforderungen zur Bekämpfung der Geldwäsche.“ (EU-Kommission 2010, Fußnote zu Klausel 5)

Hierdurch wurden jedoch mehr Fragen aufgeworfen als beantwortet, weil die „demokratischen Grundsätze“ sich an vielem messen lassen müssen, unter anderem am Ausmaß einer Maßnahme oder eines Gesetzes, das wie der Patriot Act dem europäischem Verständnis von Demokratie wohl kaum entspricht. Ebenso fehlt es an der Durchsetzbarkeit von Ansprüchen betroffener Bürger, die sich in einem demokratischen Rechtsstaat gegen willkürliche Handlungen von Geheimdiensten und Regierung gerichtlich wehren können müssen. Zwar existiert in den USA ein Gericht, das die Überwachungsaktivitäten prüfen kann: der sogenannte Foreign Intelligence Surveillance Court (FISC). Allerdings hatte das Gericht beispielsweise keinen einzigen der von der US-Regierung im Jahr 2012 gestellten Überwachungsanträge abgelehnt, was an der Effektivität des Rechtsschutzes zweifeln lässt (vgl. Kimball 2013). Es bleibt also weiterhin fraglich, ob nach dem Urteil des EUGH eine Auslegung dieser Ausnahmen in dieser Weise geboten sein kann.

Andere Datenschutzbehörden haben nicht ganz so weitreichende Aussagen über die Auswirkungen des EuGH-Urteils veröffentlicht[12]. Grundlegend wird jedoch überall klargestellt: Das Safe-Harbor-Abkommen habe keine Gültigkeit mehr; die Datenexporteure – auch die deutschen Arbeitgeber – müssten ihre Datenübermittlungsgrundlagen überprüfen; Orientierungshilfen[13] stünden zur Verfügung, die vorläufig zu Rate gezogen werden könnten; zudem gebe es eine Frist bis Ende Januar 2016, bis zu deren Ablauf die EU-Kommission gemeinsam mit den USA die EU-Standardvertragsklauseln nach den neuen Vorgaben des Urteils anzupassen habe[14]. Es bleibt also abzuwarten, wie sich die Verhandlungen bis dahin entwickeln.

12 Vgl. BfDI (2015a) www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/22_SafeHarborIstGekippt_WasNun.html?nn=5217040 [22.2.2016] und BfDI (2015b) www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/Safe-Harbor_Update%2026_10_2015_Positionspapier%20DSK.pdf?__blob=publicationFile&v=2 [22.2.2016] und Datenschutz RLP (2015) www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf [22.2.2016].

13 Beispielsweise die „Orientierungshilfe – Cloud Computing“ des Hessischen Datenschutzbeauftragten (2014) www.datenschutz.hessen.de/download.php?download_ID=318 [22.2.2016].

14 Vgl. EU-Kommission (2015) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [22.2.2016].

4.2 Weitere offene Fragen

Neben allen offenen Rechtsfragen zum Thema des internationalen Austausches von Beschäftigtendaten wird oftmals übersehen, dass auch noch andere Fragen weitgehend ungeklärt sind.

Ein Unternehmen, das essentiell darauf angewiesen ist, dass ihm seine Daten nachhaltig zur Verfügung stehen, sollte unbedingt auch bedenken, dass Cloud-Computing-Anbieter theoretisch einfach vom Markt verschwinden können. Viele kleine Anbieter werden es nicht schaffen, sich eine Position unter den „großen" Cloud-Anbietern wie Microsoft, SAP, Strato, Dropbox und anderen zu erarbeiten, die es ihnen ermöglicht, längerfristig ihre Geschäfte aufrechtzuerhalten. Was geschieht dann mit den Daten des Unternehmens? Ähnliche Fragen stellen sich auch bei der Verschmelzung von Unternehmen – so erst kürzlich geschehen, als SAP sich den Cloud-Anbieter Concur einverleibte[15]. Gleiches gilt dann auch für die Subunternehmer der Cloud-Anbieter. Betriebsräte sollten ihrer Unternehmensleitung die grundsätzliche Frage stellen: Wie deckt sie das Risiko ab, dass die Datenverfügbarkeit nicht mehr gewährleistet sein könnte? (vgl. auch Brandt 2012)

Eine ebenso legitime Frage ist, ob es tatsächliche nach dem „Gang in die Cloud" zu wesentlichen Einsparungen geführt hat, seine Beschäftigtendaten und eine entsprechende Datenverarbeitung in eine „Datenwolke" zu verlagern. Fundierte Aussagen darüber, welchen günstigen Effekt ein solcher Schritt für die IT-Kostenstruktur hat, sind zurzeit nicht zu finden. Anbieter von Online-Datenspeichern werben zwar beständig mit Wirtschaftlichkeitsargumenten, unabhängige Studien darüber, ob sich dies am Ende bewahrheitet hat, sind jedoch nicht verfügbar. Es gehört auch zu den Aufgaben der Arbeitnehmervertretungen, risikoreiche und unwirtschaftliche Ambitionen der Arbeitgeberseite aufzuzeigen und zu hinterfragen. Zumindest muss aber die Frage gestellt werden: Wann rechnet sich neben einer bereits existierenden IT-Infrastruktur im Unternehmen eine hinzukommende oder die alte Struktur ablösende Datenverarbeitung in der Cloud? Dabei sollte auch ein genaues Augenmerk auf die Frage gelegt werden: Welches Einsparpotenzial sieht der Arbeitgeber hierbei über einen mittel- oder längerfristigen Personalabbau? Dies wird zwar für die nahe Zukunft zumeist ausgeschlossen, kann aber grundsätzlich nicht verhindert werden (Konrad-Klein/Michalke (2012, S. 35).

15 Vgl. Reuters (2014), http://www.handelsblatt.com/unternehmen/it-medien/cloud-computing-sap-schliesst-milliarden-zukauf-von-concur-ab/11078104.html [22.2.2016].

In den vorliegenden Vereinbarungen war auch zu einem anderen Thema nichts zu lesen: Für die Einführung neuer Technologien ist es ratsam, eine Gefährdungsbeurteilung erstellen zu lassen, die nach § 87 Abs. 1 Nr. 7 BetrVG mitbestimmungspflichtig ist. Dies hat das BAG in zwei Entscheidungen aus dem Jahr 2004[16] klargestellt. Ob und wie sehr die durch die Cloud-Nutzung entstehenden Veränderungen der Arbeitswelt gesundheitliche Auswirkungen für die Beschäftigten haben können, kann überhaupt erst beurteilt werden, wenn hierzu Erkenntnisse erfasst werden. Hierfür ist eine Vorher-Nachher-Analyse sinnvoll.

Schließlich ist eines der offenen Probleme, die sich für die Mitarbeitervertretungen stellen, auch die Überprüfbarkeit der Angaben über die Datenverarbeitung in geografisch weit entfernten Gebieten - sei es in der Konzernzentrale, sei es beim Cloud-Anbieter selbst. Selbst wenn sich die Gremien weitreichende Prüfrechte in den Vereinbarungen zusichern ließen, indem sie auch Zu- und Durchgriffsrechte bis hin zum Cloud-Anbieter formuliert haben, ist es ein rein faktisches Problem, diese auch auszuüben. Alleine an der Tatsache, dass die meisten Mitglieder von Mitbestimmungsgremien zeitlich überproportional eingespannt sind, wird oftmals eine sachgerechte Prüfung vorhandener Sicherungsmaßnahmen beim Auftragsdatenverarbeiter scheitern. Aber auch die Beauftragung eines Sachverständigen, der entweder online im System des auftragsdatenverarbeitenden Cloud-Anbieters selbst oder sogar vor Ort, in einem der datenschutzrechtlichen „Drittstaaten" Prüfungen vornimmt, dürfte zurzeit die absolute Ausnahme darstellen. Hier ist nicht zuletzt auch die Verhandlungsmacht der Gremien gefragt, wenn es darum geht, pragmatische Lösungen zu finden, um den „auf dem Papier" – also in einer Betriebsvereinbarung – erreichte Schutz auch ausüben zu können.

16 BAG, Beschluss vom 8.6.2004 – 1 ABR 13/03 und BAG, Beschluss vom 8.6.2004 – 1 ABR 4/03.

5 ZUSAMMENFASSENDE BEWERTUNG

Diese Auswertung begann mit der Sichtung des gesamten Archivs der Hans-Böckler-Stiftung nach Vereinbarungen, die sich explizit oder „versteckt" mit dem Thema Cloud Computing beschäftigten. Recherchiert wurde in hunderten von Texten, die von den Gremien bei der Hans-Böckler-Stiftung eingereicht worden waren. Suchfilter waren Schlüsselbegriffe bekannter Cloud-Software-Anbieter oder sonstige Formulierungen, die darauf schließen lassen, dass sich die vom jeweiligen Gremium abgeschlossene Vereinbarung auf eine Materie bezieht, die bereits bei Abschluss der Vereinbarung eine Cloud-Anwendung zur Grundlage hatte oder mittlerweile hat: z. B. durch Veränderungen der in einer Vereinbarung geregelten Software hin zu cloudbasierten Lösungen. Dies ist im Rahmen der vorliegenden Veröffentlichungsreihe eine ungewöhnliche Vorgehensweise. Üblicherweise ist aus dem gut sortierten Archiv klar erkennbar, welche Betriebsvereinbarungen und sonstige Regelungen zu einem thematischen Schwerpunkt existieren. Cloud Computing stellt hier jedoch eine Besonderheit dar, weil die Gremien sich grundsätzlich zunächst mit der Software, dem Tool oder der Anwendung selbst beschäftigten und erst – wenn überhaupt – im nächsten Schritt prüfen, welche technologische Grundlage hier zusätzlich regelungsbedürftig ist. Nach abgeschlossener Recherche beruht diese Veröffentlichung nun auf einer Anzahl von 13 Vereinbarungen, die sich entweder direkt auf eine Software beziehen, die bereits in der Cloud läuft, oder die das Thema Cloud Computing in sonstiger Weise aufgreift.

Schon diese Schilderung der Recherche kann jedoch als Teil der Analyse selbst verstanden werden. Denn alleine die Tatsache, dass nach mehreren Jahren, in denen laut statistischen Erhebungen (vgl. Kapitel 1) die cloudgestützte Datenverarbeitung mehr als nur randständig Einzug in die Unternehmen gehalten hat, noch immer entsprechende Regelungen sich im Archiv nicht erkennbar häufen, lässt den Schluss zu: Hier herrscht thematisch eine große Unkenntnis oder zumindest eine große Unsicherheit.

Beobachtbar ist, dass keine der vorliegenden Vereinbarungen den Cloud-Bezug direkt aufgreift. Weiter beobachtbar ist, dass es sich bei den ausgewerteten Vereinbarungen, die verifizierbar eine cloudgestützte Software zum Thema haben, stets um zwei bis drei Anwendungen handelt, die von vielen Unternehmen eingesetzt werden. Hier ist eine Monopolisierung des Marktes zu vermuten. Dass bedeutet: Deutsche Unternehmen bevorzugen bei der Frage nach einem Vorschlag zur Lösung eines inhaltlichen Problems oftmals die

gleichen Anbieter und damit die gleichen Softwarelösungen. Warum dies so ist, kann hier nur vermutet werden – es birgt jedoch sowohl Gefahren als auch Vorteile für die Gremien:

Plant ein Unternehmen, einen bestimmten Unternehmensbereich informationstechnologisch auf eine neue Software bzw. auf ein ganzes Paket an miteinander verknüpften Anwendungen umzustellen, kann der Betriebsrat heute davon ausgehen, dass die zu regelnde Materie bereits in anderen Unternehmen in einer Vereinbarung abgebildet wurde. Dies kann durch „Netzwerken" unter den Gremien zu enormem Kenntnisgewinn und damit zu einer enormen Zeitersparnis führen. Fehlt einem Beteiligten das Hintergrundwissen, kann er sich zumindest einen Grundsachverstand bilden, indem er bereits ausformulierte Vereinbarungen zum gleichen Thema heranzieht. Dies kann dazu führen, dass zumindest eher bekannt ist, welche Schwierigkeiten auf die Mitarbeitervertretungen zukommen können. Augenscheinlich wurde diese Möglichkeit bisher jedoch noch wenig genutzt.

Der Nachteil ist das Risiko, das durch die Monopolisierung des Marktes entsteht. Würden z. B. alle deutschen Unternehmen die gleiche cloudbasierte Reiskostenabrechnungssoftware nutzen, wären binnen kürzester Zeit alle Reisen deutscher Beschäftigter bei einem einzigen Cloud-Anbieter zusammengeführt. Selbst bei umfassenden Datensicherungsmaßnahmen des Anbieters selbst würde dies eine unübersehbare Gefahr darstellen – ein Punkt, auf den Gremien bei der Mitbestimmung Wert legen sollten. Gegebenenfalls ist nicht einmal dem Unternehmer klar, welche Marktentwicklung er mit einer solchen kurzfristig getroffenen Entscheidung befördert. Hier kann der Betriebsrat mit Wissensvorsprung unterstützend eingreifen.

Ein Ergebnis der Auswertung ist zudem insbesondere die Erkenntnis, dass keine der Regelungen in der notwendigen Ausführlichkeit die hinter den geregelten Softwareeinsätzen stehenden Cloud-Lösungen thematisiert oder ansatzweise zufriedenstellend löst. Diesbezüglich kommt viel Arbeit auf die Gremien zu. Nicht nur bei neu einsetzenden Verfahren sollte künftig die Frage an den Arbeitgeber gerichtet werden: Welcher Art ist die genutzte Cloud? Die Mitarbeitervertretungen sind heute dazu aufgerufen, bestehende Anwendungen und hierzu bereits abgeschlossene Vereinbarungen daraufhin zu überprüfen, ob wesentliche Teile der mitbestimmungspflichtigen Materie übersehen wurden. Es dürfte angezeigt sein, die dabei erkennbaren und unabsichtlich ungeregelten Technologien im Rahmen eines beginnenden Datenschutz- und Mitbestimmungsmanagement einer Bearbeitung zuzuführen, die durch eine dann einsetzende Regelhaftigkeit möglichst bald zwar zu einem vergleichsweise neuen, aber beherrschbaren Teil der Betriebsratsarbeit wird.

6 BERATUNGS- UND GESTALTUNGSHINWEISE

Dieses Kapitel gibt in kompakter Form Anregungen, welche Punkte bei der Mitgestaltung von Vereinbarungen zum Thema Cloud Computing wichtig sein könnten. Das Ziel der Veröffentlichung, vorliegende betriebliche Regelungen zu analysieren und dabei einen Überblick über verbreitete Praktiken zu geben, erlaubt es nicht, allzu sehr in die Einzelheiten zu gehen. Die zahlreichen Hinweise sind in folgendem Gestaltungsraster zusammengefasst. Es handelt sich dabei nicht um einen geschlossenen Vorschlag zur unmittelbaren Anwendung, sondern um einen Stichwortkatalog zur Unterstützung eigener Überlegungen. Es ist ein Angebot, sich mögliche Regelungspunkte einer Vereinbarung noch einmal im Überblick zu verdeutlichen, um die zentralen Aspekte für die eigene Situation zu finden.

6.1 Gestaltungsraster

Gegenstand der Vereinbarung

- genaue Bezeichnung der Software inkl. Versionsnummer und Datum
- genaue Bezeichnung des Anbieters der Software
- Bezeichnung der Cloud-Lösung (SaaS, PaaS, IaaS; Privat-/Public-/Hybrid-Cloud)
- kurze/prägnante/umreißende Beschreibung des Einsatzgebietes der Software im Unternehmen
- Beschreibung, wie tiefgreifend Veränderungen am System sein müssen, um die Mitbestimmungsrechte wieder aufleben lässt (nur bei wesentlichen Veränderungen des Systems, der Cloud-Lösung, der Datenkategorien oder der Softwaremodule)
- Verweise/Anlagen: Vertrag mit Softwareanbieter, Vertrag mit Cloud-Anbieter, Benutzerhandbuch, Service Level Agreement (SLA), Pflichtenheft, technische Beschreibung des Systems, Systemarchitektur etc.

Definitionen

- Begriffsdefinitionen für die Inhalte/Zwecke des Systems
- Begriffsdefinitionen für die technischen Beschreibungen der Software und der Cloud-Lösung

Geltungsbereich

- sachlich (siehe Geltungsbereich)
- personell (Beschränkung auf notwendige Teile der Beschäftigten bzw. Einbeziehung aller Bereiche, soweit erforderlich)
- räumlich (Berücksichtigung mobiler Nutzung)

Zweck der Datenverarbeitung

- ausführliche Beschreibung des Einsatzgebietes der Software mit Bezeichnung aller einzelnen Bereiche (Reisebuchungen, Reisekostenerfassung etc.)
- Beschreibung der Erforderlichkeit (Ausnahmefall) der Datenverarbeitung in einer cloudbasierten Software; rein wirtschaftliche Erwägungen sind nicht ausreichend;
- Wahrung des Grundsatzes der Datentrennung (es sollen mit einer Software/einem System nicht alle irgend möglichen Zwecke erfüllt werden; Vermeidung von umfassenden Profilbildungen innerhalb eines Systems)
- Klarstellung der Freiwilligkeit, soweit keine erforderliche Datenerhebung erfolgt; ausführliche Schutzmechanismen beschreiben, die eine freiwillige Einwilligung ermöglicht (absolute Ausnahme)
- Verweise/Anlagen: Muster der Einwilligungserklärung für die Beschäftigten; hier muss die Tatsache der Cloud-Datenverarbeitung ausführlich beschrieben werden.

Art der Daten

- Benennung der Datenkategorien der personenbezogenen oder personenbeziehbaren Daten der Mitarbeiter, die in dieser Software verwendet werden
- Beschreibung, wie diese Daten in die Software eingespeist werden (manuelle Eingabe, Übertragung aus Stammdatensystem o. Ä.)
- ausführliche Begründung, warum genau diese Daten erforderlich sind (pro Datenkategorie)

Auswertung

- Welche Auswertungen will das Unternehmen vornehmen, um den/die oben benannten Zweck(e) zu erreichen
- Bezeichnung der technisch möglichen Auswertungen, die nicht genutzt werden (soweit diese nicht systemseits abgeschaltet werden können)
- Verweise/Anlagen: Screenshots der Reports

Verknüpfung mit anderen Systemen, Schnittstellen

- Benennung aller Schnittstellen, über die Daten in das System gelangen oder über die Daten das System verlassen
- Beschreibung der Datenkategorien pro Schnittstelle
- Ausgabestellen/-geräte erfassen

Zugriffsrechte

- Zugriffsberechtigte im Unternehmen (Funktionsbeschreibung wie Datenbankadministrator, Nutzer, Supervisor) und die jeweiligen Zugriffsberechtigungen (lesen, ändern, löschen etc.)
- Zugriffsberechtigte in angeschlossenen Unternehmenseinheiten (Konzernbeteiligte etc.)
- Zugriffsberechtigungen Dritter bzw. Auftragsdatenverarbeiter (Software-Anbieter, Cloud-Anbieter, Wartungsunternehmen, Server-Betreiber etc.)
- ggf. auf Zugriffs-/Rechtemanagementsystem im Unternehmen verweisen
- alle systemverantwortlichen Zugriffsberechtigten auf die Geheimhaltungspflichten gem. § 5 BDSG verpflichten
- Verweise/Anlagen: Rollen- und Berechtigungskonzept

Aufbewahrungsfristen, Löschfristen

- Bezeichnung der Löschfristen (falls unterschiedlich: pro Datenkategorie)
- Benennung der zwingend vorgeschriebenen Aufbewahrungspflichten inkl. gesetzlicher Vorschrift oder Begründung der tatsächlichen Notwendigkeit der Speicherdauer; Benennung gesetzlicher Vorschriften anderer Länder zu Aufbewahrungspflichten (Cloud-Anbieter in Ländern mit nicht adäquatem Datenschutzniveau)
- ggf. auf Löschkonzepte im Unternehmen verweisen (archivierte Daten etc.)

Grenzüberschreitender Datenverkehr, Konzerndatenfluss, Auftragskontrolle

- Benennung aller beteiligten Unternehmen
- Beschreibung der Datenflüsse
- Bezeichnung der erforderlichen Verträge (mit Datum der Unterzeichnung), wie Auftragsdatenverarbeitungsverträge gem. §11 BDSG, EU-Standardvertragsklauseln, Codes of Conduct
- Beschreibung der Konsequenzen eines Anbieterwechsels in einen Staat mit unsicherem Datenschutzniveau

- Beschreibung von Ausgleichsmechanismen und Abwägungskriterien (Verhältnismäßigkeitsprinzip) bei kollidierenden Rechtsvorschriften unterschiedlicher Staaten

Datensicherheit
- Datensicherheitskonzept im Unternehmen, Verschlüsselungen, Protokolldateien etc.
- Datensicherheitskonzept in verbundenen Unternehmen (Konzern)
- Datensicherheitskonzept des Cloud-Anbieters, Zertifizierungen

Leistungs- und Verhaltenskontrollen
- soweit der Zweck der Software eine von der unternehmerischen Entscheidung abhängige Leistungs- oder Verhaltenskontrolle der Beschäftigten erfordert: Benennung des Zwecks und exakte Benennung der Kontrollen (z. B. Erfassung von Arbeitszeit/Kontrolle der Einhaltung der Arbeitszeit; Erfassung der Reisekosten/Kontrolle der Budgetüberschreitung)
- ansonsten: Leistungs- und Verhaltenskontrollen ausschließen!
- insbesondere: Übernahme von Aufgaben der Strafverfolgungsbehörden durch den Arbeitgeber verbieten; Grenzen definieren (z. B. § 32 Abs. 1 Satz 2 BDSG)

Beweisverwertungsverbote
- jegliche Verwertung von zu Unrecht erhobenen Daten ausschließen
- jegliche Verwertung zu Unrecht erfolgten Auswertungen ausschließen
- jegliche Verwertung der zu Unrecht erfolgten Leistungs- und Verhaltenskontrollen ausschließen

Rechte des Betriebsrats
- gesetzliche Informationspflichten und die darüber hinausgehenden, sinnvollen weiteren Informationspflichten klarstellen
- gesetzliche und darüber hinausgehende Mitwirkungsrechte klarstellen
- Mitwirkungsrechte bei Ausnahmeregelungen beschreiben (Auswertungen, Beweisverwertung)
- Ausnahmeregelungen für Mitglieder des Betriebsrats benennen (keine Datenaufzeichnung etc.)
- anlassbezogene und anlassunabhängige Prüfrechte des Betriebsrats
- Beteiligung an Eskalationsplänen
- Auskunftspflichten des betrieblichen Datenschutzbeauftragten gegenüber dem Betriebsrat normieren

- Hinzuziehung von Sachverständigen zu Prüfungen vereinfachen
- Durchgriffsrechte des Betriebsrats zu Auftragsdatenverarbeitern normieren

Veränderung von Geschäftsprozessen, Rationalisierungsgefahr
- Beschreibung der Geschäftsprozesse, auf die der Einsatz der Software und die Verarbeitung in der Cloud kurz-, mittel- und langfristig Auswirkungen haben wird
- Gefährdungspotenzialanalyse und Prüffristen
- Ausschluss von personellen Veränderungen basierend auf dem Einsatz der Software, des Systems, der Cloud-Kapazität etc.

Schulungen, Qualifizierung
- Qualifizierung für die Bedienung des Systems/der Software innerhalb der Arbeitszeit
- Ansprechpartner benennen

Ausschluss von Risiken
- Konsequenzen für die Beschäftigten bei Systemausfall etc. ausschließen
- Arbeitnehmerhaftung begrenzen (Risiko bei konzernweitem Einsatz cloudgestützer Verfahren)

Schlussbestimmungen
- Wirksamwerden der Vereinbarungen von rechtmäßigen vertraglichen Grundlagen abhängig machen
- Konfliktregelungen, Einigungsstelle
- Kündigungsfristen, Nachwirkung
- salvatorische Klausel

6.2 Ausgangspunkte für die gestaltende Einflussnahme durch die Interessenvertretung

Wie gezeigt, findet cloudgestützte Datenverarbeitung heute in vielen Unternehmen bereits statt. Es ist jedoch aus den vorliegenden Vereinbarungen nicht ersichtlich, dass innerhalb der Gremien oder der Betriebe systematische Erwägungen stattgefunden hätten, wie mit dieser neuen Qualität der Verarbeitung von Beschäftigtendaten umgegangen werden sollte.

Vielmehr wurde die nun eingesetzte, cloudbasierte Software genauso behandelt, wie es bei der Einführung und Anwendung klassischer Datenverarbeitungsmodule zu erwarten gewesen wäre: Es wurde auf der Basis der fachlichen Gründe für den Einsatz der Software eine Betriebsvereinbarung entwickelt, die die vermeintlich fachimmanenten Risiken abfangen sollte. Demzufolge wurden also beispielsweise bei Reisekosten- oder Reisemanagement-Anwendungen eher Überlegungen angestellt, wie mit nicht ordnungsgemäßen Abrechnungen umzugehen sei. Denn in der Vergangenheit lag bei Reisekostenabrechnungen das größte Risiko eher darin, dass Mitarbeiter durch Ungenauigkeiten in den Verdacht des Betrugs gerieten, wenn ein Kostenirrtum zu ihren Gunsten vorlag. Dies hätte bzw. hat teilweise dramatische Konsequenzen bis hin zur Entlassung des entsprechenden Mitarbeiters nach sich ziehen können.

Heute hingegen liegt ein viel größeres Risiko darin, dass die entsprechenden Bewegungs- und Abrechnungsdaten innerhalb einer Cloud in Ländern verarbeitet werden, deren Datenschutzniveau nicht das des europäischen Rechtsraumes erreicht. Zwar mag es sein, dass die Konsequenzen, die ein Arbeitgeber auf eine unrichtige Reisekostenabrechnung eines Beschäftigten hin gezogen hatte, schneller und konkreter wirkten, wie zum Beispiel eine verhaltensbedingte Kündigung oder zumindest eine individualrechtliche Abmahnung. Die Tatsache jedoch, dass die Risiken einer cloudgestützten Datenverarbeitung sich gegebenenfalls erst nach langer Zeit realisieren, stellt selbst wiederum ein erhöhtes Risiko dar. Man kann sich eventuell vorstellen, dass beispielsweise ein auf dem Markt konkurrierendes Unternehmen durchaus Interesse daran haben könnte, die (Reise-)Bewegungsdaten von tausenden von Beschäftigten – über Jahre hinweg gesammelt – zu analysieren. In welche Regionen der Welt hat der Konkurrent viele Mitarbeiterreisen gezahlt? Welche Märkte hat der Konkurrent dadurch gegebenenfalls erschlossen? Oder eine viel persönlichere Analyse: Bezogen auf den einzelnen Beschäftigten kann ausgewertet werden, wer welche Vorlieben bei Dienstreisebuchung hat, ob er Diätnahrung im Hotel wünscht, ob ein Raucherzimmer angefordert wird oder ob der Beschäftigte in der ersten oder zweiten Klasse gereist ist. Die Profilbildungsmöglichkeiten sind schier unbegrenzt.

Daher muss der heutige Ansatz für die Einflussnahme der Interessenvertretungen ein anderer sein: Zunächst sollte ein Gremium bei jeder neuen IT-Anwendung die Möglichkeit in Betracht ziehen, dass es sich um eine cloudgestützte Datenverarbeitung handelt und den an den Arbeitgeber gerichteten Fragenkatalog darauf zuschneiden. Dies setzt natürlich voraus, sich zunächst einmal das Wissen um die Besonderheiten der unterschiedlichen Cloud-

Lösungen anzueignen. Da die Risiken vermehrt in der Art der Datenverarbeitung zu suchen sind, muss hierauf auch mehr Wert beim Abfassen und Verhandeln der Vereinbarung gelegt werden. Hierdurch verändert sich die Sichtweise auf scheinbar risikoärmere oder risikoreichere Verhandlungsmaterie. Waren früher eher die Menge und Qualität der personenbezogenen Daten, die tatsächlich im System erfasst wurden, ein Indiz für ein erhöhtes Risiko, so ist nun auch oder vor allem das System selbst immer mehr das Risiko. Die Fragen nach den weltweiten Zugriffsmöglichkeiten und -berechtigungen, nach der Dauer der Datenspeicherung oder nach gesetzlichen Vorgaben in Ländern, in denen die Cloud auf Server zugreift, werden immer entscheidender. Insbesondere nach dem EuGH-Urteil zur Aufkündigung des Safe-Harbor-Abkommens stehen cloudbasierte Anwendungen mehr und mehr im Fokus der Datenschützer.

Betriebsräten ist insoweit anzuraten, den Einzelfalllösungen systematische, übergreifende Regelungen voranzustellen. So sollten die internationalen Datenströme einer generellen Lösung zugeführt werden. Mit dem Verständnis auf der Arbeitgeberseite, dass dies mittelfristig Zeit und Geld spart, kann hier auf freiwilliger Basis eine bzw. können mehrere Rahmenregelungen geschaffen werden, die den Abschluss von internationalen Verträgen zum Datentransfer zwischen den Unternehmen und internationalen Auftragsdatenverarbeitern regeln. Es kann Einfluss auf die Auswahl der Cloud genommen werden oder zumindest auf die Auswahl und Inhalte der Vertragslösungen, je nachdem, ob es um einen konzerninternen Datenfluss geht oder externe Dritte vertraglich gebunden werden sollen (Codes of Conducts, Binding Corporate Rules, EU-Standardvertragsklauseln). Auf dieser Grundlage lassen sich cloudgestützte Anwendungen besser eingrenzen, die eigentlichen Verwendungsgründe der so genutzten Software einfacher darstellen und die wesentlichen Veränderungen (Versionswechsel, Updates) besser regelmäßig nachverhandeln. Vielleicht müssen sich die Gremien künftig auch darauf konzentrieren, eine Phase der Vorarbeiten zu überstehen, in der sie modulhaft einzelne Bestandteile von Vereinbarungen (Leistungs- und Verhaltenskontrollen, Rechte des Betriebsrats u. a.) in einer Art Baukastenprinzip bevorraten. Aus diesem „Bausatz" lassen sich dann künftig unter Bezugnahme auf eine Rahmenvereinbarung, schneller und pragmatischer Vereinbarungen zusammensetzen und auf diese Art selbst komplizierte Regelungsmaterien abbilden. Die Arbeit der Gremien wird sich in jedem Fall mittelfristig verändern müssen, um die vielfältiger werdende Materie der dynamischen Datenverarbeitung von Beschäftigtendaten in Clouds besser fassen und regeln zu können.

6.3 Wesentliche rechtliche Grundlagen

Die rechtliche Behandlung von Softwareanwendungen im Unternehmen unterliegt datenschutzrechtlich verschiedenen Gesetzen. Zunächst ist hier grundlegend das Bundesdatenschutzgesetz (BDSG) zu nennen, das in vielen seiner Vorschriften beispielsweise die Grundsätze des Datenschutzrechts normiert. Diese kommen bei jedem Einsatz von Softwareanwendungen im Unternehmen zur Anwendung. Bei cloudgestützer Softwareanwendung ist dies nicht anders. Allerdings muss bei Cloud-Verfahren systematisch auf einer anderen Ebene der Regelungsmaterie begonnen werden, eine rechtliche Einordnung vorzunehmen. Denn da das BDSG vorgibt, dass jedwede Datenverarbeitung personenbezogener Daten auf eine rechtliche Grundlage zu stützen ist, müssen hier entweder Rechtsvorschriften oder Einwilligungen der Betroffenen vorliegen – und das auch auf internationaler Ebene. Im Arbeitsverhältnis ist jedoch die Einwilligung ein sehr Bedenkliches Instrument, da aufgrund des Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer davon auszugehen ist, dass es an der Freiwilligkeit der Einwilligung mangelt. Es bleiben also nur gesetzliche oder sonstige Rechtsvorschriften zur Rechtfertigung der Datenverarbeitung.

Kann man sich bei unternehmensinternem Softwareeinsatz direkt und ausschließlich auf die bundesdeutschen Vorschriften stützen, finden die meisten cloudgestützten Verarbeitungen von Beschäftigtendaten in Datenwolken statt, die nicht über bundesdeutschem Gebiet schweben, sondern z. B. über den USA. Die Folge ist, dass zunächst der Weg, den die Daten in und aus unserem rechtlichen Hoheitsgebiet nehmen, abgesichert werden muss. Immer wenn die Datenverarbeitung in einem Land (oder mehreren Ländern) stattfindet, dessen (deren) Regelungen nicht dem europäischen Datenschutz adäquat gegenüberstehen, spricht man von einem Land „ohne adäquates Datenschutzniveau“. Bei einer hier stattfindenden Verarbeitung von Beschäftigtendaten würden die Unternehmen diese einem höheren Risiko aussetzen, als es der europäische Datenschutzstandard vorsieht. In diesem Fall muss der Schutz der Daten anderweitig erreicht werden.

Hierfür sind, wie bereits im Eingangskapitel beschrieben, verschiedene Lösungsmodelle vorhanden. Ein Datenaustausch erfolgt grundsätzlich durch den Abschluss von Verträgen zwischen den jeweiligen Daten austauschenden Unternehmen selbst; oder das externe Unternehmen beruft sich auf ein Zertifikat, das gleiches beinhaltet. Allerdings können die Unternehmen solche Verträge nicht unkontrolliert abschließen bzw. werden nicht jedwede Arten von Zertifikaten akzeptiert. Damit die jeweiligen Verträge und Zertifikate in

ihrer Regelungsschärfe auch das notwendige Schutzniveau erreichen, gibt es Abkommen, die beschreiben, was ein solcher Vertrag alles zu enthalten bzw. was ein solches Zertifikat inhaltlich nachzuweisen hat.

Beispielsweise existierte das sogenannte Safe Harbor Abkommen, auf dessen Grundlage sich die Unternehmen zertifizieren lassen konnten, um so zu belegen, dass sie sich an den europäischen Vorgaben streng orientierten. Dieses Zertifikat galt dann durch Vorlage an den europäischen Auftraggeber sowie durch weitere Maßnahmen als Basis für die Datenverarbeitung. Durch das Urteil des EuGH vom 6.10.2015 hat dieser das Abkommen jedoch für obsolet erklärt, weil es nach Ansicht des EuGH den gewollten rechtlichen Schutz nicht gewährleisten konnte. Alle auf der Grundlage dieses Abkommens stattfindenden Datenübermittlungen sind damit datenschutzrechtlich nicht mehr gerechtfertigt.

Es existieren jedoch weitere rechtfertigende Möglichkeiten für den internationalen Datenaustausch. So hat die EU sogenannte Standardvertragsklauseln verabschiedet, die die Daten austauschenden Unternehmen unterzeichnen können. Halten sie sich an die Vorgaben, ist der Datenverkehr legitimiert. Die EU-Standardvertragsklauseln dürfen in ihrem Wortlaut nicht verändert werden, weil sie nur so die Einhaltung des Schutzniveaus garantieren können. Werden die Texte verändert, muss dies erneut von einer Datenschutzaufsichtsbehörde genehmigt werden. Eine weitere Möglichkeit ist die Erstellung sogenannter Codes of Conduct (oder vergleichbar auch Binding Corporate Rules), in denen sich ein konzernangehöriger Auftragsdatenverarbeiter in einem Land mit nicht adäquatem Datenschutzniveau den europäischen Datenschutz- und Datensicherheitsstandards unterwirft. Da letzteres jedoch zunächst auf freiwilliger Basis geschieht, ist vor einer etwaigen Genehmigung durch die Datenschutzaufsichtsbehörden nicht zwingend davon auszugehen, dass dies in jedem Fall eine entsprechende Absicherung darstellt.

Hat man die rechtlichen Grundlagen für den internationalen Datenaustausch geschaffen, müssen weitere gesetzliche Vorgaben erfüllt werden. Das BDSG gibt in § 3a vor, dass das Unternehmen von sich aus – das heißt ohne, dass dies von den betroffenen Beschäftigten kontrolliert werden müsste – so wenig Daten wie möglich in einer cloudbasierten Software über den einzelnen Arbeitnehmer verarbeitet. Dabei sind auch „indirekte" Daten über die Mitarbeiter relevant: Informationen darüber, mit welchen IP-Adressen sich Angestellte des Unternehmens in die Cloud einloggen, sind ebenso relevante personenbezogene bzw. -beziehbare Daten wie Informationen über die Dauer der Nutzung der Software, den Benutzernamen ebenso wie über Kommunikationsinhalte oder geografische Standortinformationen.

Die in einem solchen System erfassten und verarbeiteten Daten dürfen nach dem Zweckbindungsprinzip dann auch nur für denjenigen Zweck genutzt werden, für den sie ursprünglich vorgesehen waren. Gleiches gilt für die Dauer der Datenspeicherung. Nur so lange die Daten für den vorgesehenen Zweck in der Cloud erforderlich sind, dürfen sie dort vorgehalten werden. Alle weiteren Datenschutzgrundsätze gelten also in der Cloud genauso, wie auch bei standortbasierten Systemen. Bei der Betrachtung der gesetzlichen Grundlagen für die Verarbeitung von Beschäftigtendaten kommt allumfassend auch wieder § 32 BDSG zum Einsatz. Jedwede Begründung für die Verarbeitung derlei Daten in cloudgestützten Verfahren muss sich daran orientieren, ob die so verarbeiteten Daten der Mitarbeiter für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses notwendig ist. Dabei handelt es sich nicht um eine frei zu bestimmende Datenmenge, die beispielsweise für die „Durchführung" des Beschäftigungsverhältnisses genutzt werden kann. Die Vorgaben sind sehr eng und orientieren sich stets am datenschutzrechtlichen Begriff der Erforderlichkeit.

Problematischer wird es dann, wenn die cloudgestützte Datenverarbeitung Teile enthält, die eine laufende Kommunikation darstellen (z. B. Chat-Funktion). Ist hierbei beispielsweise auch eine private Nutzung der entsprechenden Anwendung erlaubt, kommt das Telekommunikationsgesetz (TKG) und damit das Fernmeldegeheimnis (§ 88 TKG) zur Anwendung. Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz schützt aber auch bereits die dienstlichen Kommunikationsdaten.

Eine abschließende Liste einschlägiger Gesetze, die für die cloudgestützte Datenverarbeitung relevant ist, kann hier nicht erstellt werden, da stets die sehr individuellen Softwarelösungen und deren Vielfältigkeit Ausgangspunkt für eine rechtliche Einordnung sind. Gremien liegen aber in ihrer Einschätzung sicherlich nicht falsch, wenn sie sich zunächst an den auch für die Einführung standortbasierter Softwareanwendungen orientieren und dann die zumeist vorliegende Internationalität der Cloud-Basis zusätzlich rechtlich absichern.

Schwierig wird es hierbei, die Rechte anderer Staaten in die die Überlegungen mit einzubeziehen. Zumeist hat das Gremium jedoch den Vorteil, dass die Cloud-Anbieter bereits selbst die für sie einschlägigen Gesetze geprüft und in ihren Geschäftsbedingungen ausgestaltet haben. So kann man bei der Geltung aller einschlägigen Gesetze daran anknüpfen, wie die Vorgaben des deutschen Rechts mit den vom Cloud-Anbieter geforderten rechtlichen Rahmenbedingungen zusammenpassen. Es kann hierbei zu Rechte-

kollisionen kommen – ein deutscher Arbeitgeber sowie auch die Betriebsräte müssen bei der Zusammenführung zweier Rechtsmaterien innerhalb einer Betriebsvereinbarung grundlegend das allgemeine Persönlichkeitsrecht des einzelnen Beschäftigten heranziehen, insbesondere den Verhältnismäßigkeitsgrundsatz für die Interessenabwägung auf Rechtsebene.

7 BESTAND DER VEREINBARUNGEN

Die vorliegende Auswertung basiert auf 13 Vereinbarungen aus dem Gesamtbestand des Archivs Betriebliche Vereinbarungen der Hans-Böckler-Stiftung.

Tabelle 1

Art und Anzahl der Vereinbarungen

Art der Vereinbarung	Anzahl
Betriebsvereinbarung	3
Gesamtbetriebsvereinbarung	3
Konzernbetriebsvereinbarung	1
Ergänzungs-Gesamtbetriebsvereinbarung	1
Dienstvereinbarung	1
Europäische Betriebsvereinbarung	1
Regelungsabrede	1
Richtlinie	2
Gesamt	**13**

Tabelle 2

Verteilung der Vereinbarungen nach Branchen

Branche	Anzahl
Gesundheit und Soziales	1
Öffentliche Verwaltung	1
Chemische Industrie	1
Maschinenbau	2

Großhandel (ohne Kfz.)	1
Mess-, Steuerungs- und Regelungstechnik	1
Anonym	1
Börse/Makler	3
Fahrzeughersteller von Kraftwagenteilen	1
Nachrichtentechnik/Unterhaltungs-, Automobilelektronik	1
Gesamt	**13**

Tabelle 3

Abschlussjahr der Vereinbarungen

Abschlussjahr	Anzahl
2009	1
2010	2
2011	1
2012	4
2013	3
2014	2
Gesamt	**13**

LITERATUR- UND INTERNETVERZEICHNIS

Literatur

Beuth, Patrick (2015): Der EuGH hat ein Monster erschaffen, Zeit online, 8.10.2015, Download unter http://www.zeit.de/digital/datenschutz/2015-10/safe-harbor-eugh-konsequenzen [14.2.2016].

Bitkom e.V. (2014) (Hg.): Nutzung von Cloud Computing in Unternehmen wächst, Presseinformation vom 30.1.2014, Download unter www.bitkom.org.

Bitkom Research GmbH (2015): Cloud-Monitor 2015, Studie im Auftrag der KPMG AG, Download unter www.bitkom.org.

Brandt, Jochen (2012): Cloud Computing – Lohnt sich der Griff nach den Wolken?, in: Computer und Arbeit, Ausgabe 5/2012, S. 27–28.

Bundesamt für Sicherheit in der Informationstechnik – BSI (Hg.) (2012): Sicherheitsempfehlungen für Cloud Computing Anbieter, Eckpunktepapier, Download unter www.bsi.bund.de.

Bundesministerium für Wirtschaft und Technologie (2012): Das Normungs- und Standardisierungsumfeld von Cloud Computing. Eine Untersuchung aus europäischer und deutscher Sicht unter Einbeziehung des Technologieprogramms „Trusted Cloud", Download unter www.bmwi.de.

Datenschutz RLP (2015): Der Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (Hg.) (2015): Folgerungen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz aus dem Urteil des EuGH vom 6. Oktober 2015 (C-362/14) „Safe Harbor", veröffentlicht am 26.10.2015, Download unter www.datenschutz.rlp.de.

Der Hessische Datenschutzbeauftragte (Hg.) (2014): Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Version 2.0, Stand 9.10.2014, Download unter https://www.datenschutz.hessen.de.

Die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) (Hg.) (2015a): Safe Harbour ist gekippt – was nun?, Pressemitteilung vom 26.10.2015, Download unter www.bfdi.bund.de.

Die Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) (Hg.) (2015b): Safe Harbor – Update (26.10.2015), Positionspapier der Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder, Download unter www.bfdi.bund.de.

Dr. Datenschutz (2013): Cloud-Computing: Neuer Algorithmus revolutioniert Verschlüsselung, Download unter www.datenschutzbeauftragter-info.de/cloud-computing-neuer-algorithmus-revolutioniert-verschluesselung/ [14.2.2016].

Europäische Kommission (Hg.) (2010): Beschluss der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, Aktenzeichen K(2010) 593 (2010/87/EU), Download unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:DE:PDF [14.2.2016].

Europäische Kommission (Hg.) (2015): Statement of the Article 29 Working Party, Brussels, 16 October 2015, Download unter http://ec.europa.eu.

Heidemann, Robert (2012): Beratung zum Einsatz von Cloud Computing bei einem Maschinenbauer in Mittelhessen, in: Technologieberatungsstelle beim DGB Hessen (Hg.) (2013): Tätigkeitsbericht 2012, http://tbs-hessen-thueringen.de [14.2.2016].

Kimball, Spencer (2013): Kritik an US-Geheimgericht FISC", Deutsche Welle 14. 7.2013, Download unter http://dw.com/p/196qZ [14.2.2016].

Kirsch, Christian (2011): US-Behörden dürfen auf europäische Cloud-Daten zugreifen, Download unter www.heise.de/ix/meldung/US-Behoerden-duerfen-auf-europaeische-Cloud-Daten-zugreifen-1270455.html [14.2.2016].

Konrad-Klein, Jochen/Michalke, Friedhelm (2012): Virtualisierung + Cloud Computing, Reihe: Arbeit, Gesundheit, Umwelt, Technik, Heft 73, Technologieberatungsstelle beim DGB NRW e.V. (Hg.), Download unter www.tbs-nrw.de/fileadmin/Shop/Broschuren_PDF/TBS_Cloud_virtualisierung.pdf [14.2.2016].

Lehmann, Michael/Giedke, Anna (2013): Cloud Computing – technische Hintergründe für die territorial gebundene rechtliche Analyse, in: Computer und Recht (CR) 9/2013, S. 608–616.

Mielchen, Daniela (2013): Verrat durch den eigenen Pkw – Wie kann man sich schützen?, in: Zeitschrift Straßenverkehrsrecht (SVR) 3/2014, S. 81 (85, 87).

Reuters (2014): SAP schließt Milliarden-Zukauf von Concur ab, Online-Meldung am 5.12.2014, in: Handelsblatt online, Download unter www.handelsblatt.com.

Ruchhöft, Matthias (2012): Virtualisierung und Cloud Computing, BTQ Kassel (Hg.), Download unter https://www.btq-kassel.de/upload/m50922764c9a96_verweis1.pdf [14.2.2016].

Schröder, Christian/Spies, Axel (2014): „USA: Vorlage von E-Mails an US-Behörden, die auf Servern in Irland gespeichert sind – Neue Gefahren für US-Clouds?", in: ZD-Aktuell 2014/03194, Download unter https://beck-online.beck.de.

Statistisches Bundesamt (2014): 12 % der Unternehmen setzen auf Cloud Computing, Pressemitteilung vom 19.12.2014 - 467/14, Download unter www.destatis.de.

Stuckmann, Heike u. a. (2012): Claus der Cloudworker, Kurzfilm-Beitrag zum Thema Cloud Working, verdiTV 5.4.2012, www.verdi.de/verdi.tv [14.2.2016].

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) (Hg.) (2015): Positionspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14, veröffentlicht am 14.10.2015, Download unter www.datenschutzzentrum.de.

Wedde, Peter (2014): Cloud Computing, in: Computer und Arbeit 7–8/2014, S. 14–18.

Internethinweise

Das Statistik-Portal Statista bietet diverse Statistiken zur Nutzung von Cloud Computing in Unternehmen in Deutschland: www.statista.com.

Ein Beratungsangebot der Gewerkschaft ver.di für Cloud-Worker findet sich seit diesem Jahr unter: www.cloudworker-beratung.de.

Auch die IG Metall bietet eine Plattform zum Thema Crowdwork: www.faircrowdwork.org.

Urteile und Beschlüsse

BAG, Beschluss vom 8.6.2004 – 1 ABR 13/03

BAG, Beschluss vom 8.6.2004 – 1 ABR 4/03

EuGH, Urteil vom 6.10.2015, C-362/14

ÜBER DIE SAMMLUNG VON BETRIEBSVEREINBARUNGEN

Die Hans-Böckler-Stiftung verfügt über die bundesweit einzige bedeutsame Sammlung betrieblicher Vereinbarungen, die zwischen Unternehmensleitungen und Belegschaftsvertretungen abgeschlossen werden. Derzeit enthält unsere Datenbank etwa 16.000 Vereinbarungen zu ausgewählten betrieblichen Gestaltungsfeldern.

Unsere breite Materialgrundlage erlaubt Analysen zu betrieblichen Gestaltungspolitiken und ermöglicht Aussagen zu Trendentwicklungen der Arbeitsbeziehungen in deutschen Betrieben. Regelmäßig werten wir betriebliche Vereinbarungen in einzelnen Gebieten aus. Leitende Fragen dieser Analysen sind: Wie haben die Akteure die wichtigsten Aspekte geregelt? Welche Anregungen geben die Vereinbarungen für die Praxis? Wie ändern sich Prozeduren und Instrumente der Mitbestimmung? Existieren ungelöste Probleme und offene Fragen? Die Analysen betrieblicher Vereinbarungen zeigen, welche Regelungsweisen und -verfahren in Betrieben bestehen. Die Auswertungen verfolgen dabei nicht das Ziel, Vereinbarungen zu bewerten, denn die Hintergründe und Strukturen in den Betrieben und Verwaltungen sind uns nicht bekannt. Ziel ist es, betriebliche Regelungspraxis abzubilden, Trends aufzuzeigen und Gestaltungshinweise zu geben.

Bei Auswertungen und Zitaten aus Vereinbarungen wird streng auf Anonymität geachtet. Die Kodierung am Ende eines Zitats bezeichnet den Standort der Vereinbarung in unserem Archiv und das Jahr des Abschlusses. Zum Text der Vereinbarungen haben nur Mitarbeiterinnen und Mitarbeiter des Archivs und Autorinnen und Autoren Zugang.

Zusätzlich zu diesen Auswertungen werden vielfältige anonymisierte Auszüge aus den Vereinbarungen in der Online-Datenbank im Internetauftritt der Hans-Böckler-Stiftung zusammengestellt. Damit bieten wir anschauliche Einblicke in die Regelungspraxis, um eigene Vorgehensweisen und Formulierungen anzuregen. Darüber hinaus gehen wir in betrieblichen Fallstudien gezielt Fragen nach, wie die abgeschlossenen Vereinbarungen umgesetzt werden und wie die getroffenen Regelungen in der Praxis wirken.

Das Internetangebot ist unmittelbar zu erreichen unter
www.boeckler.de/betriebsvereinbarungen

Anfragen und Rückmeldungen richten Sie bitte an
betriebsvereinbarung@boeckler.de