„Outsourcing“ Datenschutz bei der Einführung Workday – ein Change-Erfahrungsbericht

Knut Hüneke
Vortrag auf der 33. Konferenz für Mitarbeitervertretungen
Neue Technologien und Datenschutz
09. – 11. November 2021 in München

Zu meiner Person

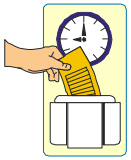
Knut Hüneke
Diplom-Psychologe
Arbeits-, Betriebs- und Organisationspsychologie
Beratung, Training, Organisationsentwicklung

Mathias-Duschl-Str. 5e
D-82140 Olching
+49 81 42 ... Fon: 284 56 80
Fax: 284 56 81

Mobil: +49 172 82 22 365
e-mail: k.hueneke@link-m.de
http://www.khueneke.link-m.de

- Diplom-Psychologe, Schwerpunkt Arbeits-, Betriebs- und Organisationspsychologe
- 1991 – 1993 Unternehmensberatung in München
- Seit 1993 freiberuflich tätig
- 2009 – 2017 Qualitäts- und Prozessmanager sowie Organisationsentwickler in Krankenhäusern in Thüringen

- Seit 2018 Projektmanager im POR der LHM



- Lebe in Olching bei München
- Weitere Infos sowie Links zu meinen diversen Veröffentlichungen:
  www.khueneke.link-m.de

Was will ich euch heute berichten?

- Zum Verständnis der Situation: Das Unternehmen
- Herausforderungen
  - International agierender Konzern
    – will personalwirtschaftlich und IKT-technisch entsprechend aufgestellt sein
- Wie der BR bisher agiert hat
- An welche Grenzen der BR dabei kam
  - Komplexität und Aufwand für Datenschutz
  - Kollektivvereinbarung als Rechtsgrundlage
- Piloter „Outsourcing“ Datenschutz
  - Neue Spielregeln durch die DSGVO
  - 1. Gehversuch: O365
  - 2. Gehversuch: Workday
- Lessons learnt
  - Beim AG
  - Beim GBR
- Fazit

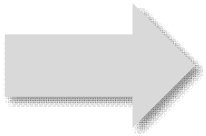
Das Unternehmen

- Marktforschung
- Internationaler Konzern
- Sitz in London
- über 100 Standorte weltweit
- >100.000 Beschäftigten
- Seit 1998 vier Besitzerwechsel
- Unzählige Reorganisationsprogramme, Umstrukturierungen …
- 1998: 7 Standorte in D mit rd. 2.000 MA*innen
- 2021: 4 Standorte in D mit rd. 1.400 MA*innen

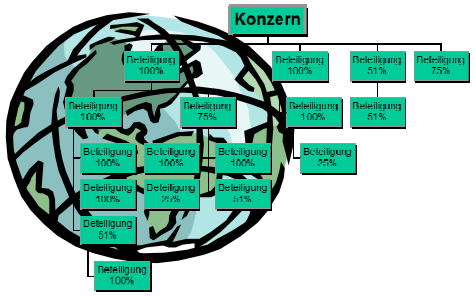
Herausforderung

Seit dem Wechsel vom

eigentümergeführtem Unternehmen



internationalem Konzern



tut die Spitze alles, um den Konzern international aufzustellen.

Weil

- (zunehmend) multi-/ internationale Projekte
- globale Konzerne als Kunden
- Betrachtung globaler Märkte

⇨Aufbau zentrale Steuerung/ Controlling

⇨Vereinheitlichung operativer Prozesse/ Standardisierung

⇨Zentralisierung Unterstützungsprozesse

⇨konzernweit die gleiche IKT

⇨zentralisierte IKT

⇨konzerneinheitliche HR/ HR-Daten

Personalwirtschaftliche Sicht

- Wer kann es (Qualifikation und Erfahrung)?
- Wer kann es „gut“?
- Wer ist verfügbar?
- Wo ist/ wer kann es am billigsten?

⇨ **Least Cost Working**

generell & konkret

– Funktionen/ Rollen
– Scales
– Wissensmanagement
– Transparenz (Kosten, Speed, Qualität, …)
– …

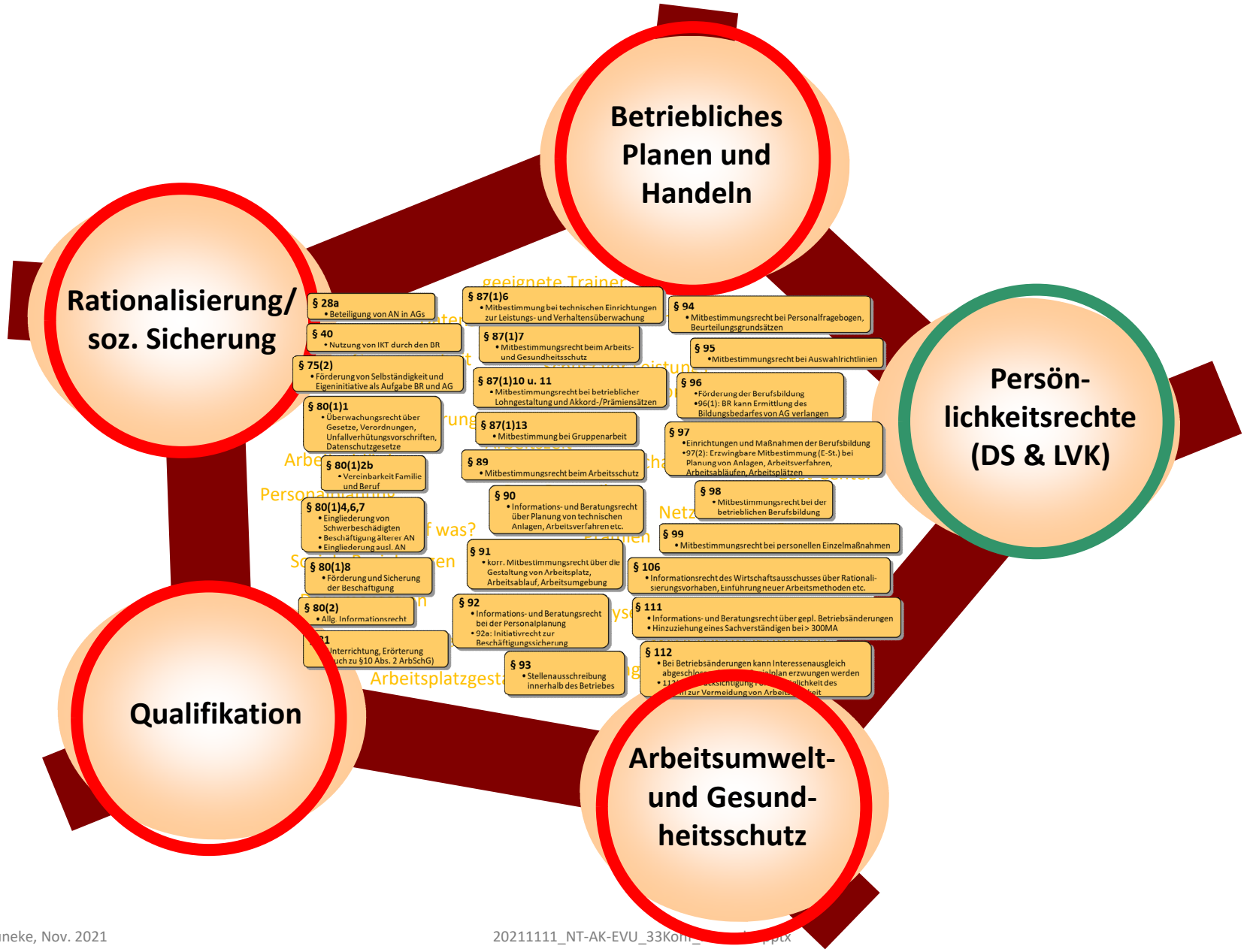
– Qualifikationen
– Erfahrung
– Beurteilung
– „Störungen“
– …

IKT-Sicht

- Outsourcing Systemverwaltung und Betrieb auf globalen Dienstleister
- konzernweit die gleiche IKT
  - Eliminierung eigener Anwendungen
    → Verlust regionaler/ nationaler Spezifika und Erfahrung
- konzerneinheitliche (Daten-)Definitionen
- konzernweit die gleichen Prozesse
- vergleichbare Standards (Benchmarks, Hitlisten, …)
- On Premise/ in eigener Regie → (globale) Clouds/ SaaS
- Business Intelligence

Wunsch: Zugriff auf Alles für Alle …

Die bisherige Linie des BRs: Konzentration auf DS und LVK



Strategie des BRs über DS & LVK

- Abkapselung D
  - Keine Zugriffe von außerhalb D
    - außer aggregiert/ anonymisiert
    - insb. für Controlling und HR
  - Aber zugleich internationales Geschäft ermöglichen
    - internationale Teams und internationales Management erfordern z.T. globale Zugriffe
    - ⇨Knifflige Ausdifferenzierung operative Zugriffe vs. Zugriffe aus anderen Zwecken
- Hebel: Datenschutz und
  Schutz vor unerlaubter Leistungs- und Verhaltenskontrolle

⇨Konsequenz

- Extrem hohe Aufwände, global-einheitliche und zunehmend als SaaS angebotenen Systeme entsprechend zuzurichten
  - Sonderlösungen je System erdenken und durchsetzen
    - für Speicherorte, Rollen, Berechtigungen, Reports, …
  - Verknüpfungen beschränken und monitoren
    - Schnittstellen, ETL-Prozesse, BI/BO, …

Hebel Datenschutz: zunehmend komplex und kaum noch handhabbar

- Standarddatenschutzmodell*
  - Datenminimierung
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Nichtverkettung
  - Transparenz
  - Intervenierbarkeit
- EU-Standardvertragsklausel für Non-EU-Datenverkehr
- Orientierungshilfe Cloud-Computing DSB-AK_TuM**
- BSI Anforderungskatalog Cloud-Computing
  - z.B. Mandantenfähigkeit, wie sie z.B. im BSI-Grundschutz M 2.549 thematisiert wird
  - z.B. Transfer-Verschlüsselung vs. e2e-Verschlüsselung
- Speziell USA: Cloud-Act & Co
- …

Zudem: großes Unverständnis und hohe Widerstände beim Konzern

*Zu finden unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0a.pdf
**Zu finden unter https://www.datenschutzkonferenz-online.de/media/oh/20141009_oh_cloud_computing.pdf

Dilemma: Regelung schafft Rechtsgrundlage

- Wir wollen/ müssen unseren Kolleg*innen ermöglichen, ihre Arbeitsleistung zu erbringen die sie dem AG schulden ... und damit mittelbar dafür sorgen, dass sie bezahlt werden können ;-)
  → System (geregelt) zulassen, BV abschließen
- Aber mit einer BV schaffen wir zugleich die Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten gemäß
  - § 26 Abs. 4 BDSG,
  - Art. 9 Abs. 2 lit. b) DSGVO
  - Art. 88 Abs. 1 DSGVO
- Also:
  - ☹ Wir regeln O365 und haben damit eine Rechtsgrundlage geschaffen für die Datenverarbeitung, obwohl wir der Meinung sind, O365 kann nicht ds-konform betrieben werden …
  - ☹ Wir schließen eine WD-BV ab und legitimieren die Personaldaten-Verarbeitung, z.T. die Verarbeitung von besonderer Kategorien von P-Daten in einer (US-)Cloud …

Vertiefung: Rechtsgrundlage gem. § 26 Abs. 4 BDSG

(Hervorhebung durch den Autor)

(4) „Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von **Kollektivvereinbarungen** zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.“

Vertiefung: Rechtsgrundlage gem. Art. 88 DSGVO, Datenverarbeitung im Beschäftigungskontext (Hervorhebung durch den Autor)

(1) „Die Mitgliedstaaten können durch Rechtsvorschriften oder durch **Kollektivvereinbarungen** spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch **Kollektivvereinbarungen** festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

(2) Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, **die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben**, und die Überwachungssysteme am Arbeitsplatz.“

Vertiefung: Rechtsgrundlage gem. Art. 9 Abs. 2 b) DSGVO, Verarbeitung besonderer Kategorien personenbezogener Daten

(Hervorhebung durch den Autor)

(1) [Die Verarbeitung besonderer Kategorien personenbezogener Daten ist untersagt.]

(2) „Absatz 1 gilt nicht in folgenden Fällen:

a) (…)

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer **Kollektivvereinbarung** nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,“

c) (…)

Mit der DSGVO haben sich die Spielregeln verändert

- Höheres Bewusstsein für DS beim AG, auch international
  - ob positiv oder negativ spielt keine Rolle
- scharfes Schwert Bußgeld
  - bis zu 20Mio. €/ max. 4% Jahresumsatz
  - das immer öfter „niedersaust“*
- zugleich hohe Unsicherheit
  - noch keine Grundsatzurteile für das Beschäftigungsverhältnis
  - wegweisende und als "radikal" wahrgenommene Urteile aus anderen Bereichen
    - Schrems I und II, ...
      - Safe Harbour gekippt
      - EU-Standardvertragsklauseln "kippelig" bzw. konkret auszufüllen

*s. https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php

1. Gehversuch zum DS-“Outsourcing“: O365

- 2-teilige Regelung
  - Teil 1, Allgemeine Regelungen, Basis- und Gruppenfunktionalitäten
  - Teil 2, Regelungen zu den Analytics-Funktionen

- Problem
  - Der Konzern hat so eingekauft, dass nur ein Tenant eingerichtet werden kann, also weltweit gelten die gleichen Systemeinstellungen
  - Eine globale Deaktivierung der Analytics-Funktionen oder Azure-Speicherung ist nicht durchsetzbar
  - Bliebe nur, den Einsatz von O365 in D zu untersagen …

- Lösung
  (vor dem Hintergrund einer Ein-Tenant-Installation)
  - Individuelle Nutzung der Analytics-Funktionen erlaubt, da nicht zu verhindern
  - Verbot der Nutzung der Analytics-Funktionen durch Arbeitgeber
  - Vorbehaltliche Zustimmung des GBRs

Vertiefung 1/3 zu O365:
Nutzungs*erlaubnis* für Analytics-Funktionen für die Kolleg*innen …

„2.1 Office Graph und Delve

2.1.1 Solange Office Graph und Delve nicht durch Einrichtung eines eigenen Tenants für Deutschland oder auf Ebene der Gruppe oder anderweitig deaktiviert werden können, wird vereinbart:

Gefährdungsmitteilung an User*innen

(a) Für alle bereits erteilten Accounts von Office 365 wird eine zwischen Arbeitgeber und GBR einvernehmlich bestimmte und mit dem bDSB XY D abgestimmte Information an diese Nutzer übermittelt, in der

- die Nutzer über die Funktion von Delve detailliert informiert werden,
- die Gefährdungen für die Persönlichkeitsrechte anschaulich dargestellt werden
- die Rechtsauffassung des GBRs bezüglich anlassloser Vorratsdatenspeicherung sowie Widerspruch zum Gebot der Nicht-Verkettung dargelegt und
- die Möglichkeit der Deaktivierung und eine Anleitung zur Deaktivierung bzw. Aktivierung und sensiblen Handhabung gegeben wird.

Deaktivierung als Default

(b) Für alle zukünftig neuen Office 365-Accounts wird die individuelle Deaktivierung dieser Funktionen gem. Art. 25 DSGVO als Default eingestellt und zusätzlich die unter Ziff. 2.1.1(a) Information zur Verfügung gestellt. Der Arbeitgeber verpflichtet sich, falls durch Systemwartungen oder Updates diese Default-Einstellungen überschrieben werden, diese nachzupflegen.

2.1.2 Es erfolgt keine Kontrolle, inwieweit einzelne Anwender und in welchem Umfang diese Funktionen abgeschaltet bzw. konfiguriert haben.

2.1.3 Sofern möglich soll eine aggregierte Übersicht über die individuellen Einstellungen sowie den Nutzungsumfang der Analytics-Funktionen erstellt und dem GBR regelmäßig zur Verfügung gestellt werden (zweimal pro Jahr).“

Vertiefung 2/3 zu O365:
… plus Nutzungs*verbot* für Analytics-Funktionen für den Arbeitgeber

„2.2 Nutzungseinschränkung für Office Graph und alle weiteren Analytics-Funktionen

2.2.1 Delve ist neben den Einschränkungen gem. Ziffern 2.1.1(a) und 2.1.1(b) nur für die Nutzung auf Gegenseitigkeit unter den Kolleg*innen zugelassen und dies auch nur unter Vorbehalt (Ziff. 2.3).

2.2.2 Darüberhinausgehende analysierende Funktionen wie My Analytics, Workplace Analytics und die API-Schnittstelle für Office Graph sind deaktiviert bzw. werden, sollte dies nicht möglich sein, nicht genutzt.

2.2.3 Damit sind dem Arbeitgeber (inkl. Vorgesetzte der diversen Ebenen) jegliche Auswertungen von Daten zur Leistungs- und Verhaltenskontrolle, die auch nur in Teilen auf Daten auf Basis Office Graph oder den Analytics-Funktionen zugreifen, untersagt. Selbst beiläufig/ zufällig erlangte Kenntnisse dürfen in keiner Weise zum Nachteil der Arbeitnehmer verwendet werden (Verwertungsverbot für unzulässig erlangte Tatsachen). Personelle Maßnahmen, die auf Informationen beruhen, die unter Verstoß gegen diese GBV gewonnen wurden, sind unwirksam.“

Vertiefung 3/3 zu O365: … plus *vorbehaltliche Zustimmung* des GBRs

„2.3 Vorbehaltlichkeit der Zustimmung des GBRs

2.3.1 Es wird hiermit ausdrücklich betont, dass der GBR mit diesen unter Ziffern 2.1 und 2.2 dieser Vereinbarung gemachten Zugeständnissen in keiner Weise die Verhältnisse akzeptiert oder einer nicht-datenschutzkonformen Nutzung der Anwenderdaten durch Analytics & Co zustimmt.

2.3.2 Mit diesen Regelungen beugt sich der GBR bis zu einer weiteren Klärung, ggf. auch durch Beschreitung des Rechtsweges, lediglich der „Macht des Faktischen“ und ermöglicht den Einsatz der Basis-, Gruppen- sowie Compliance-/ IT-Security-Funktionalitäten als erforderliches Arbeitsmittel der Arbeitnehmer.“

2. Gehversuch zum DS-“Outsourcing“: Workday

- 2-teilige Regelung
  - GBV nebst Anlagen (zunächst/ derzeit nur zu Core HCM und Recruiting)
  - Zusätzlich separate Regelungsabrede Datenschutz
- GBV als Rechtsgrundlage der Datenverarbeitung ausdrücklich verneint
- Zur Sicherheit: Gesonderte Regelungsabsprache zur Wahrnehmung der Kontrollrechte des GBRs in Sachen DS gem. §80(1)1 BetrVG
  - Vorlage DSFA
    - mit Stellungnahme des bDSB oder zertifizierte Stelle
  - Vorlage Einschätzung zu Schremms I & 2 (internationaler Datenverkehr …)
    - mit Stellungnahme des bDSB oder zertifizierte Stelle
  - Bei ds-relevanten Erweiterungen oder Änderungen Workday oder besonderen Anlässen (Vorkommnisse oder Rechtsprechung) ist (neue) ds-rechtliche Bewertung vorzulegen
  - 1x/a ds-relevanter Austausch zu Workday zw. AG, GBR und bDSB
  - Weicht der AG von Empfehlung bDSB bzw. oder zertif. Stelle ab, ist dies schriftlich zu begründen und es greift Konfliktregelungsverfahren (=Einigungsstellen-fähig!)

Vertiefung 1/3 zu Workday: GBV keine Rechtsgrundlage

- „Die Gesamtbetriebsvereinbarung wird ausschließlich zur Ausgestaltung der Mitbestimmung, insbesondere gemäß § 87 Abs. 1 Nr. 6 BetrVG geschlossen und stellt keine Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten gemäß § 26 Abs. 4 BDSG, Art. 9 Abs. 2 lit. b), Art. 88 Abs. 1 DS-GVO dar.“

Vertiefung 2/3 zu Workday: gesonderte Regelungsabrede zum Datenschutz (1/2)

- „Der GBR hat sich in der GBV zur Einführung und Nutzung von Workday vom heutigen Tage erstmals und auch nur versuchsweise begrenzt auf Workday einer zeitlich vorgeschalteten detaillierten Prüfung des Datenschutzes enthalten und dies dem Arbeitgeber (Verantwortlicher gem. Art. 4 Nr. 7 DS-GVO) überlassen.
- Um dem GBR die Überprüfung der Einhaltung des BDSG und der EU-DS-GVO gemäß § 80 Abs. 1 Ziffer 1 und Abs. 2 BetrVG zu ermöglichen, werden dem GBR folgende Unterlagen zur Verfügung gestellt:
  a) Der GBR erhält vor der Einführung von Workday in Deutschland eine entsprechend aktualisierte Datenschutzfolgeabschätzung (DSFA) des Verantwortlichen.
  b) Zusätzlich oder integriert in die DSFA erhält der GBR eine Einschätzung des Verantwortlichen zur Verarbeitung personenbezogener Daten von Beschäftigten des Arbeitgebers in Ländern außerhalb des Geltungsbereichs der DS-GVO bzw. gleichgestellter Länder vor dem Hintergrund der sog. Schrems-Urteile I & II EuGH.
  c) Bei datenschutzrelevanten Änderungen und/oder Erweiterungen von Workday oder auf Grund von sonstigen besonderen Anlässen (z.B. ds-relevanten Vorfällen, Änderung der Rechtsprechung/ neue Urteile) ist dem GBR eine entsprechende datenschutzrechtliche Bewertung des Verantwortlichen zu dieser Änderung vorzulegen.“

Vertiefung 3/3 zu Workday: gesonderte Regelungsabrede zum Datenschutz (2/2)

- „Bei der Erstellung der aktualisierten DSFA sowie weiterer datenschutzrechtlicher Bewertungen nach vorstehenden lit. (a) bis (c) ist eine schriftliche Stellungnahme des betrieblichen Datenschutzbeauftragten (bDSB) oder einer im Datenschutzrecht anerkannten/zertifizierten Institution vorzulegen.
- Einmal jährlich hat, unabhängig von einer Aktualisierung der DSFA oder aktueller Bewertungen, ein Austausch zu datenschutzrechtlichen Fragen im Zusammenhang mit der Nutzung von Workday zwischen dem Arbeitgeber, dem GBR und dem bDSB zu erfolgen.
- Weicht die Arbeitgeberin in der Praxis von einer Empfehlung, der Bewertung oder der Stellungnahme nach vorstehenden lit. (c) ab, ist das schriftlich zu begründen. In diesen Fällen gilt das Konfliktregelungsverfahren der IKT-RGBV.“

Lessons learnt beim Arbeitgeber

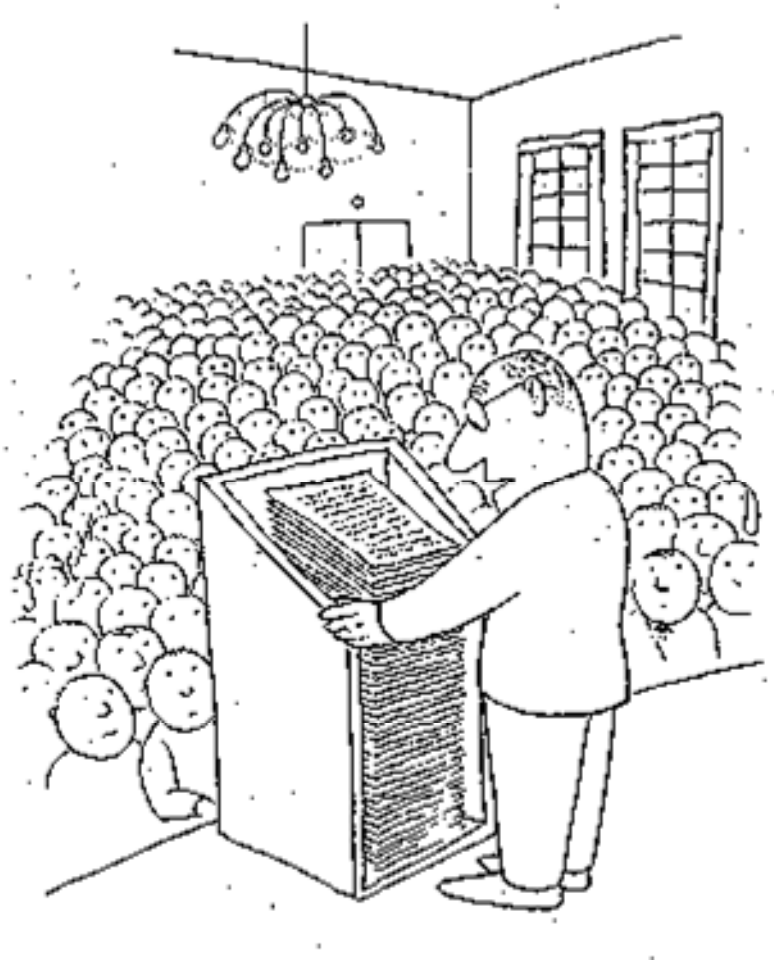
- Der deutsche Arbeitgeber war zunächst überfordert
- hat sich spezialisierte anwaltliche Beratung geholt
- die dem Arbeitgeber klar gemacht hat:
  - Du trägst die Verantwortung
  - kannst dich jetzt nicht mehr auf eine GBV als Rechtsgrundlage zurückziehen
  - sondern musst selbst abwägen und Workday ds-konform gestalten bzw. Abweichungen fundiert begründen
  - sonst droht Bußgeld
- Der Arbeitgeber D hat das als Risiko an die Konzernmutter gemeldet
  - die das Risiko als hinreichend ernst zu nehmen eingeschätzt,
  - sich erstmals ernsthaft über eine ds-konforme Gestaltung eines Systems Gedanken gemacht bzw. an einer entsprechenden Ausgestaltung aktiv mitgewirkt und
  - und dies auch entsprechend umgesetzt hat … wenigstens ansatzweise.

Lessons learnt beim GBR

- Loslassen fällt schwer
  - Als Bestimmungen aus der GBV oder deren Anlagen in der DSFA als Belege für einen ds-konformen Einsatz von WD angeführt wurden, witterten viele Kolleg*innen „verrat/ verschaukeln/ ...“
  - Aber: Wenn über §87(1)6 BetrVG z.B. Hitlisten/ vergleichende Auswertungen oder der Zugriff auf bestimmte Informationen jenseits FK und FK2 ausdrücklich verboten sind, dann kann das natürlich auch zu Recht in der DSFA als „Pluspunkt“ vermerkt werden
  - Und umgekehrt: Die Forderungen des GBRs zum Schutz vor LVK tragen zu einem ds-konformen Betrieb bei, der das Risiko des AGs reduziert
- Der GBR kann die DSFA und die zugehörigen Stellungsnahmen nur zur Kenntnis nehmen. Wenn der Arbeitgeber bereit ist, das damit verbundene Risiko zu tragen, dann liegt das alleine in dessen Verantwortung
  - Dem GBR bleibt im Rahmen seiner Überwachungsrechte nach §80(1)1 BetrVG am Ende nur, ggf. bei der Aufsichtsbehörde zu intervenieren – was der AG wiederum in seine Risikobewertung einfließen lassen sollte …

Fazit

- Die Verantwortung für den DS liegt beim Verantwortlichen
  - Dadurch haben sich erstaunliche Lerneffekte beim Arbeitgeber eingestellt
- Es konnte ein regelmäßiges Monitoring zum DS etabliert werden
- LVK zu regeln bleibt Aufgabe für den GBR: z.B. bei der Frage des Zugriffs durch Projektleitungen aus verbundenen Konzernunternehmen im Ausland, Schnittstellen, Reports etc.
- Aber in Fragen des internationalen Zugriffs, Cloudproblematik, Verschlüsselung etc. ist der GBR deutlich entlastet (Verantwortung)
  – wenn er manchmal auch noch hadert (Folterwerkzeuge fehlen)
- Für den weiteren Ausbau von Workday über Core HCM und Recruiting hinaus sowie andere Systeme bleibt abzuwarten, ob sich das „Outsourcing“ bewährt:
  - Bleibt die „Aktivierung“ des AGs in Sachen DS nachhaltig?
  - Wie bewähren sich die Aktualisierungen oder die jährlichen Gespräche zum Datenschutz?
  - Vermissen wir in Zukunft doch noch den „Hebel“ Datenschutz?
    - ⇨Aber wir können für neue Regelungen fallweise oder generell wieder zurück
    - ⇨Und auch Workday kann da, wo die Musik drin ist, wieder zurückgeholt werden



Ich danke für Eure Aufmerksamkeit