I.M.U.
Institut für Mitbestimmung und Unternehmensführung

Das I.M.U. ist ein Institut der Hans-Böckler-Stiftung

BETRIEBS- UND DIENSTVEREINBARUNGEN

Nr. 020 · März 2023 · Hans-Böckler-Stiftung

TRANSPARENTE UND BESCHLEUNIGTE IT-EINFÜHRUNGSPROZESSE (2023)

Beispiel aus der Praxis

Holger Bargmann

www.betriebsvereinbarung.de

Quelle: Konzernbetriebsvereinbarung „Rahmenvereinbarung IT Datenverarbeitungssysteme“

→| Unternehmensbezogene Dienstleistungen, 09.02.01/632/2018

Darum geht es:
Bei der Evaluation aller abgeschlossenen IT-Betriebsvereinbarungen kam der Betriebsrat des Unternehmens zu dem Ergebnis: Viele Regelungen sind veraltet und eine Vielzahl immer gleicher Formulierungen zieht sich durch alle Vereinbarungen. Daraus entstand die Idee, eine IT-Rahmenvereinbarung abzuschließen. Vorrangige Ziele: die Zahl der abzuschließenden Vereinbarungen reduzieren, die Bearbeitung beschleunigen und dabei stets die Mitbestimmung des Betriebsrats sicherstellen. Grundlage dafür war die Entwicklung einer Checkliste, die mehrere Funktionen gleichzeitig erfüllt: rechtzeitige Information, die Dokumentation der Systeme und die Freigabe durch den Betriebsrat. Verlinkt wurde diese Checkliste mit dem Verarbeitungsverzeichnis, das damit zu einem wirksamen Kontrollinstrument des Betriebsrats wurde.

Diese Vereinbarung ist keine Mustervorlage. Vorgestellt wird ein verhandelter und abgeschlossener Kompromiss. Die anonymisierten Auszüge aus abgeschlossenen Vereinbarungen werden von Kolleginnen und Kollegen aus Betriebs- bzw. Personalräten sowie der zuständigen Gewerkschaften kommentiert und ggf. von weiteren Expertinnen und Experten eingeordnet.

Kontakt
Ansprechpartner/in für dieses Beispiel: Nils Werner
betriebsvereinbarung@boeckler.de

Inhalt

Quelle: Die Kennung bezeichnet die Quelle, das Jahr des Abschlusses und den Standort im Archiv der Hans-Böckler-Stiftung.

→I Unternehmensbezogene Dienstleistungen, 09.02.01/632/2018

1 Ausgangssituation

2014/2015 evaluierte der EDV-Ausschuss des Konzernbetriebsrats (KBR) die vorhandenen Betriebsvereinbarungen und deren Handhabung in der betrieblichen Praxis. Das Ergebnis: Viele Vereinbarungen waren veraltet, bezogen sich nicht mehr auf vorhandene Systeme, die Formulierungen enthielten viele Überschneidungen und Doppelungen. Kontrastiert wurden die Ergebnisse dieser Evaluation mit einer Analyse der damaligen Konzernsituation: zunehmend globale Ausrichtung aller Prozesse, zunehmende Digitalisierung und damit einhergehend zunehmendes Einführen von IT-Systemen. Die Arbeitsweise der IT-Abteilung orientiert sich an einem standardisierten Projektmanagementkonzept, das unternehmensintern als „Architectural Review“ bezeichnet wird. In dessen Rahmen spielen Checklisten für die systematische Abarbeitung aller erforderlichen Schritte eine zentrale Rolle. Dieses Grundkonzept eines Vorgehensmodells nahm der KBR als Blaupause und passte es an die Zwecke der Information und Beteiligung des Betriebsrats (BR) bei der Einführung von IT-Systemen an. Diese Betriebsrats-Checkliste wurde zum integralen Bestandteil der Verhandlungen einer IT-Rahmenvereinbarung. Da keine Vorläuferversion existierte, musste ein vollständig neues Konzept entwickelt werden. Primäre Ziele des Betriebsrats: zum einen die Mitbestimmungsprozesse beschleunigen, vor allem durch Reduzieren der abzuschließenden Betriebsvereinbarungen und Verkürzen der Bearbeitungszeiten; zum anderen den Datenschutz stärken. Die etwa ein Jahr dauernden Verhandlungen führten 2015 zu einem ersten Abschluss einer Rahmenvereinbarung, die 2018 aktualisiert und auf der Grundlage der Datenschutzgrundverordnung (DSGVO) erweitert wurde.

„Wir sind in einer agilen Kultur, und durch die Checklisten ist es uns möglich, gemeinsam schneller zu handeln. Auch hier verfolgten wir mit dem Arbeitgeber ein gemeinsames Ziel: Die Daten aller Mitarbeiter zu schützen. Die Verhandlungen waren kontinuierlich und konsensorientiert, wie bei uns üblich.“ (Betriebsrätin, Vorsitzende des EDV-Ausschusses des Konzernbetriebsrats)

Für die Verhandlungen erhielt der EDV-Ausschuss Übertragungsbeschlüsse aller Standortbetriebsratsgremien in Deutschland, einschließlich der Abschlussvollmacht. Die Verhandlungsfortschritte und Zwischenergebnisse wurden vom EDV-Ausschuss kontinuierlich mit den lokalen Gremien und dem Konzernbetriebsrat abgestimmt sowie auf der Betriebsräteversammlung einem größeren Kreis präsentiert.

2 Umsetzungspraxis

Jedes IT-Projekt wird im EDV-Ausschuss anhand der vereinbarten Checkliste vorgestellt, einschließlich der Anforderungen des Datenschutzbeauftragten. Auf dieser Grundlage entscheidet der EDV-

Ausschuss, ob die Checkliste, die gleichzeitig die Funktionen Information, Dokumentation und Freigabe beinhaltet, für das jeweilige IT-System ausreicht oder ob eine eigenständige Betriebsvereinbarung zu verhandeln ist. Dieser Prozess gilt nicht nur für die Einführung neuer Systeme, sondern auch für Änderungen existierender Systeme im Rahmen von Erweiterungen oder Releasewechseln. Die Entscheidungen darüber trifft der EDV-Ausschuss.

In Unternehmen mit lokalen Betriebsratsgremien, Gesamt- und Konzernbetriebsräten ist die Zuständigkeit für die Ausübung der Mitbestimmung im Betriebsverfassungsgesetz (BetrVG) in § 50 für den Gesamtbetriebsrat und in § 58 für den Konzernbetriebsrat geregelt. GBR und KBR sind immer dann die zuständigen Träger der Mitbestimmung, wenn mehrere Betriebe bzw. Standorte betroffen sind und das Thema aus zwingenden Gründen nicht auf lokaler Ebene geregelt werden kann. Der EDV-Ausschuss kann nur dann rechtsgültige Mitbestimmungsentscheidungen – hier: die Freigabe von Systemänderungen – fällen, wenn der KBR ihn mittels entsprechender Beschlüsse beauftragt.

Der EDV-Ausschuss wurde von den lokalen Gremien und dem Konzernbetriebsrat durch Delegationsbeschlüsse mandatiert, für die zuletzt genannten Themen rechtsgültig die Mitbestimmung auszuüben. Dadurch werden Instanzenwege sachlich und zeitlich deutlich abgekürzt und die Mitbestimmungsprozesse beschleunigt. Eine solche Übertragung von Entscheidungsbefugnissen an einen Ausschuss setzt ein hohes Maß an Vertrauen voraus – eine Voraussetzung, die in diesem Unternehmen besteht. Wie bei der Verhandlung der IT-Rahmenvereinbarung werden auch über Themen und Beschlüsse des EDV-Ausschusses regelmäßig der KBR, die lokalen Gremien und die Betriebsräteversammlung informiert.

„Im KBR besteht Einigkeit, dass IT immer alle unsere deutschen Standorte betrifft. Daher agieren wir hier im EDV-Ausschuss mit Vertretern der Standorte.“ (Betriebsrätin, Vorsitzende des EDV-Ausschusses des Konzernbetriebsrats)

Für eine zuverlässige und schnelle Abstimmung zwischen dem EDV-Ausschuss und den lokalen Gremien sowie GBR und KBR ist eine Zusammensetzung förderlich, welche die einzelnen Standorte ebenso abbildet wie eine gewisse Heterogenität hinsichtlich IT-Kompetenzen, Mitbestimmungserfahrung und Technikaffinität, die den Blickwinkel erweitert.

Eigenständige Betriebsvereinbarungen werden nur in Ausnahmefällen und für komplexe und weitreichende IT-Systeme abgeschlossen, wobei die

Regelungen der Rahmenvereinbarung stets die Grundlage bilden. Dieser Weg wurde z. B. gewählt für das Personalmanagementsystem Workday und für Office 365.
Arbeitgeber und Betriebsrat verständigten sich, für bestimmte Anwendungsfälle, für die verschiedene IT-Systeme mit gleichen oder sich überschneidenden Funktionalitäten auf dem Markt verfügbar sind, nicht mehr systemspezifische, sondern technikunabhängige Regelungen zu vereinbaren. Dies gilt z. B. für Ticketsysteme.
Für die Überprüfung, ob faktisch nur IT-Systeme mit einer Freigabe durch den Betriebsrat betrieben werden, dient gemäß Artikel 30 DSGVO das Verarbeitungsverzeichnis. Dieses ist in dem Unternehmen sehr ausführlich dargestellt mit allen erforderlichen Detailinformationen sowie der hinterlegten Checkliste. Der Betriebsrat hat einen autonomen Online-Zugriff, nicht nur auf das Verzeichnis selbst, sondern auch auf alle relevanten IT-Systeme mit personenbezogenen (Beschäftigten-)Daten.
In einer internen Präsentation werden die Erfahrungen des Betriebsrats mit den Regelungen der Rahmenvereinbarung und deren Umsetzung wie folgt zusammengefasst:

- schnellere und frühe Einbindung des BR durch konsequente Einbindung der Checkliste in die Projektsteuerung
- höherer Wissensstand zu aktuellen IT-Systemen seitens BR und KBR
- gleichzeitig Einbindung des Datenschutzbeauftragten
- BR und KBR sind schneller entscheidungs- und handlungsfähig
- Lernprozess für beide Seiten über die letzten Jahre
- weniger Vereinbarungen, aber mehr Arbeit durch die Zahl der Checklisten.

3 Konzernbetriebsvereinbarung „Rahmenvereinbarung IT Datenverarbeitungssysteme“

→| Unternehmensbezogene Dienstleistungen, 09.02.01/632/2018

„[…]

2. Präambel

[…]
[Das Unternehmen] und [der] Konzernbetriebsrat sind sich darüber einig,
[…]

3. dass durch IT-Systeme generierte Informationen nicht dazu geeignet sind, Menschen und ihr Verhalten umfassend zu beurteilen oder zu kontrollieren,
4. dass IT-Systeme als die Arbeit unterstützende Hilfsmittel eingesetzt werden,
5. dass Arbeitsabläufe unter Anwendung gesicherter arbeitswissenschaftlicher Erkenntnisse so gestaltet werden müssen,

dass Entscheidungsspielräume erhalten bleiben und Über- oder Unterforderungen der Beschäftigten vermieden werden.

Die Regelungen zum Erhalt von Handlungs- und Entscheidungsspielräumen sowie zur Vermeidung von Über- und Unterforderung der Beschäftigten sind nicht nur im Zusammenhang mit qualifikationshaltigen Arbeitsstrukturen und Gesundheitsschutz (Vermeidung von Monotonie) relevant. Die aktuelle Debatte um die „Bändigung" der künstlichen Intelligenz geht ebenfalls in diese Richtung: Die IT-Systeme sollen den Werkzeugcharakter behalten und die Menschen bei der Arbeit unterstützen, nicht sie bevormunden und als Anhängsel der Technik behandeln. Die Algorithmen sollen keine autonomen Entscheidungen treffen, sondern diese den Menschen überlassen.

3. Zielsetzung

Ziele dieser Betriebsvereinbarung sind:

1. dass die Einführung, Nutzung und spätere Anpassung von Systemen der Informationstechnik konstruktiv von Arbeitgeber, Konzern- und Standortbetriebsrat und Beschäftigten begleitet wird,
2. sicherzustellen, dass die Leistungs- und Wettbewerbsfähigkeit [des Unternehmens] erhöht wird und zukunftssichere Arbeitsplätze erhalten bzw. geschaffen werden,
3. sicherzustellen, dass die einschlägigen nationalen und europäischen Gesetze und Bestimmungen, insbesondere das Bundesdatenschutzgesetz (BDSG), das Arbeitsschutzgesetz (ArbSchG), die Bildschirmarbeitsverordnung (BildschArbV) und das Betriebsverfassungsgesetz (BetrVG) eingehalten werden,
4. sicherzustellen, dass das individuelle Recht der Beschäftigten auf informationelle Selbstbestimmung gewährleistet wird, und dass die Interessen der Beschäftigten in angemessenem Umfang berücksichtigt werden,
5. sicherzustellen, dass der Betriebsrat seine gesetzlichen Mitbestimmungsaufgaben rechtzeitig und in angemessenem Umfang wahrnehmen kann.

4. Allgemeines

Begriffsbestimmungen
Unter IT-Systemen werden sowohl Hardware, Software als auch darauf ablaufende Prozesse zur Datenverarbeitung jeglicher Art verstanden.
Unter Daten über das Verhalten oder die Leistung von Beschäftigten werden alle Informationen verstanden, die Aussagen darüber erlauben, was Beschäftigte zu einem bestimmten oder unbestimmten Zeitpunkt getan oder unterlassen haben.

Alle Informationen, die Aussagen über das Verhalten oder die Leistung von Beschäftigten geben, gehören zu den personenbezogenen Daten im Sinne des Art. 4 DSGVO. Dies sind insbesondere auch solche Daten, die durch IT- oder andere Systeme erzeugt, verarbeitet und gespeichert werden und Zwecken des Datenschutzes oder der Sicherstellung des ordnungsgemäßen Betriebs des Systems dienen.
Personenbezogene Daten i. S. d. Art. 4 DSGVO sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
Verarbeiten von Daten ist jedes Eingeben, Ermitteln, Speichern, Verändern, Übermitteln, Sperren, Löschen, Auswerten und Lesen von Daten gemäß Art. 4 DSGVO.
Alle personenbezogenen Daten sind allein oder im Zusammenhang mit anderen Informationen geeignet, Aussagen, Prognosen oder Beurteilungen über das Verhalten oder die Leistungen der Personen abzugeben. Insofern sind alle technischen Einrichtungen, die personenbezogene Daten erfassen, speichern, verarbeiten oder ausgeben, technische Einrichtungen zur Verhaltens- und Leistungsüberwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG.

„Über die Auslegung dieser Begriffsbestimmungen gab es immer mal wieder Diskussionen, z. B. im Zusammenhang mit unserem CRM-System [= Customer Relations Management = Vertriebssystem]. Hier mussten Änderungen an Berichten vorgenommen werden. Auch die Nutzung von Servicedesk-Berichten muss immer wieder diskutiert werden.“ (Betriebsrätin, Vorsitzende des EDV-Ausschusses des Konzernbetriebsrats)

5. Arbeitnehmerüberwachung und Datenschutz

Die Verarbeitung personenbezogener Daten muss [den] Grundsätze[n] der Zweckbindung, der Transparenz und der Verhältnismäßigkeit sowie der Datensparsamkeit entsprechen.
Jeder Mitarbeiter hat das Recht der Information gem. Art. 15 DSGVO, welche personenbezogenen Daten das Unternehmen speichert und verarbeitet.

6. Verzeichnis von Verarbeitungstätigkeiten zur Zweckbestimmung und Umfang der Speicherung von Daten über Beschäftigte

Alle Konzerngesellschaften führen ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO und gewähren dem jeweiligen Betriebsrat Einsicht in das interne detaillierte Verzeichnis von Verarbeitungstätigkeiten. Das Verzeichnis von Verarbeitungstätigkeiten ist ein konzernweites Online Tool (siehe Anlage 1).
Die Erfassung, Speicherung, Verarbeitung und Nutzung personenbezogener Daten darf nur im Rahmen konkreter

Zweckbestimmungen stattfinden. Die Zweckbestimmungen müssen festgelegt sein, bevor personenbezogene Daten erfasst werden.
Der Arbeitgeber ist dafür verantwortlich, dass eine Aufstellung sämtlicher IT-Systeme, in und mit denen personenbezogene Daten der Beschäftigten erfasst, gespeichert, verarbeitet oder genutzt werden, erstellt wird. Diese Aufstellung wird um die Informationen, was erfasst und gespeichert wird, zu welchem Zweck die Daten verarbeitet oder genutzt werden dürfen, und wer Zugriff auf diese Daten hat, ergänzt.
Die Aufstellung erfolgt durch ein Verzeichnis von Verarbeitungstätigkeiten.
Der Arbeitgeber stellt sicher, dass neben diesem Verzeichnis von Verarbeitungstätigkeiten oder über dieses Verzeichnis von Verarbeitungstätigkeiten hinaus keine weiteren personenbezogenen Daten der Beschäftigten erfasst, gespeichert, verarbeitet oder genutzt werden.
Im Verzeichnis von Verarbeitungstätigkeiten sind auch die Daten aufzuführen, die von IT-Systemen erzeugt werden und Zwecken des Datenschutzes oder der Sicherstellung des ordnungsgemäßen Betriebs des jeweiligen Systems dienen.

Diese Regelung verdeutlicht: Auch personenbezogene Daten, die das System selbst im Hintergrund fortlaufend erzeugt und speichert, gehören zu den schützenswerten und im Verarbeitungsverzeichnis zu dokumentierenden Daten. Diese Kategorie von Daten, wie z. B. Logdaten mit User-ID und Zeitstempel, Protokolleinträge über die durch den Nutzer aufgerufenen Seiten und durchgeführten Transaktionen im System etc., sind hinsichtlich einer umfassenden Möglichkeit zur Leistungs- und Verhaltenskontrolle sogar wesentlich aussagefähiger als die Stammdaten eines Beschäftigten – siehe dazu die Erforderlichkeit der Beteiligung des Betriebsrats bei der Einsichtnahme und Auswertung dieser Daten (vgl. Punkt 7).

Bei Einführung neuer Systeme ist sicherzustellen, das Verzeichnis von Verarbeitungstätigkeiten zu ergänzen sowie bei Änderung bestehender Systeme entsprechend anzupassen. Änderungen bzgl. der Führung des Verzeichnisses von Verarbeitungstätigkeiten bedürfen einer einvernehmlichen Regelung der Anlage 1 zwischen Arbeitgeber und Konzernbetriebsrat.

Die Einhaltung dieser Regelung wird sichergestellt durch die im Unternehmen gewählte Struktur des Verarbeitungsverzeichnisses, das die Checkliste mit der dokumentierten Freigabe umfasst. Dieses Verknüpfen gesetzlicher Datenschutzregelungen mit der dokumentierten Ausübung der betrieblichen Mitbestimmung geht über die Vorschriften des Artikels 30 DSGVO deutlich hinaus.

7. Verhaltens- und Leistungskontrollen und Beurteilungen

Daten, die durch Systeme gleich welcher Art entstehen und die Aussagen über das Verhalten oder die Leistung von Beschäftigten erlauben, dürfen nicht zu Verhaltens- oder Leistungskontrollen oder -beurteilungen verwendet werden. Solche Informationen dürfen keinesfalls als Begründung oder Anlass für personelle Maßnahmen verwendet werden. Durch technische Einrichtungen gewonnene Informationen sind als Beweismittel bei rechtlichen Streitigkeiten nicht zulässig.
Davon ausdrücklich ausgenommen sind Zeit- und Projektzeiterfassungssysteme und die Beurteilung eines Mitarbeiters durch von ihm manuell eingegebene oder geänderte Daten in Zusammenhang mit täglichen Arbeitsprozessen, die durch IT-Systeme unterstützt werden, insofern die Arbeit im IT-System einen wesentlichen Bestandteil des Aufgabenbereiches des Mitarbeiters darstellen und die Qualität der Arbeit nur in Zusammenhang mit dem IT-System bewertet werden kann.

Diese Regelung, vor allem der zweite Teil, betrifft die systematische Grauzone zwischen kollektivrechtlicher mitbestimmungspflichtiger (nicht: verbotener!) Leistungs- und Verhaltenskontrolle und der individualrechtlich zulässigen und mitbestimmungsfreien Leistungs- und Verhaltenskontrolle durch die Vorgesetzten. Welche Daten aus welchen Quellen darf der Vorgesetzte kennen und verwenden, ohne gegen die Mitbestimmungsrechte des Betriebsrats zu verstoßen? Diese Regelung schafft Klarheit: manuell durch den Beschäftigten selbst eingegebene oder veränderte Daten, die seine Kernaufgaben betreffen – also keine systemseitig automatisch erzeugten Daten und keine solchen, die von Dritten über den Beschäftigten eingegeben werden wie z. B. in Personalmanagementsystemen.

Darüber hinaus können nur in begründeten Ausnahmefällen Systemdaten nach Zustimmung und in enger Kooperation mit dem lokalen Betriebsrat zur Unterstützung einer Verhaltens- oder Leistungsbewertung genutzt werden.
Werden in personenübergreifenden Anwendungssystemen persönliche Daten verwendet, die von mehreren Anwendern eingesehen werden können, so sind sie so zu definieren, dass keine verhaltens- oder leistungsbezogenen Rückschlüsse auf Einzelpersonen durch Dritte gezogen werden können. Dies beinhaltet auch Rückschlüsse auf sensible Mitarbeiterdaten durch Sachbearbeiter ohne direkte Personalverantwortung für einen Mitarbeiter. Davon ausgenommen sind Mitarbeiter der Personalabteilung und des Betriebsrats.
Jeder Beschäftigte muss darüber informiert werden, wann, wie und durch welche IT-Systeme sein Verhalten oder seine Leistung überwacht werden kann. Eine heimliche Überwachung findet nicht statt. Auf technische Einrichtungen, die der Kontrolle der Mitarbeiter dienen könnten, muss deutlich hingewiesen werden.

Dies betrifft in erster Linie den Einsatz von Sicherheitssoftware, die zum Schutz der Unternehmensnetze gegen Hacker und Schadsoftware zwingend erforderlich ist. Dabei finden umfassende Prüfungen und Protokollierungen im Unternehmensnetz statt, die zwangsläufig das Verhalten der Beschäftigten aufzeichnen und auswerten. Der zulässige Nutzungszweck ist Schutz, der mögliche, aber unzulässige Nutzungszweck ist Leistungs- und Verhaltenskontrolle. Da die Sicherheitssoftware als Hintergrundprozess eingesetzt wird, ist diese – meist werden mehrere Produkte parallel genutzt – für die Beschäftigten nicht sichtbar. Darum ist es erforderlich, dass über diese Systeme und die damit verbundene Überwachung informiert wird. Andernfalls wäre das Transparenzgebot des Artikels 5 DSGVO verletzt.

Sonderfälle, in denen eine Überwachung des Verhaltens von Beschäftigten aus wichtigen Gründen notwendig ist, müssen mit dem jeweiligen lokalen Betriebsrat vereinbart und mit ihm gemeinsam gehandhabt werden. Der jeweilige Betriebsrat muss immer über das Ergebnis der Überwachung informiert und angehört werden, bevor dieses Ergebnis verwendet werden kann.

In Punkt 7 ist umfänglich geregelt, welche Formen von Leistungs- und Verhaltenskontrolle stets, also in jedem IT-System, zulässig sind und welche nicht. Im vorstehenden Abschnitt wird der Umgang mit Ausnahmefällen geregelt, in denen Abweichungen von sonst unzulässigen Auswertungen möglich sein sollen. Angeknüpft wird damit an die gesetzlichen Regelungen des § 26 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes (BDSG): Sie erlauben einen Zugriff auf Beschäftigtendaten immer dann, wenn plausible Verdachtsmomente hinsichtlich strafrechtlich schwerwiegender Verstöße vorliegen. Diese gesetzliche Regelung hat Vorrang vor einer Betriebsvereinbarung. Der vorstehende Abschnitt öffnet die möglichen Fälle, also z. B. für weniger schwerwiegende Verstöße gegen das Gesetz, den Arbeitsvertrag oder gegen Compliance-Regelungen. Eine derartige Überprüfung ist jedoch ausschließlich im Vieraugenprinzip und im Konsens mit dem lokal zuständigen Betriebsrat zulässig.

Zugriff auf personenbezogene Daten kann auch durch Internal Audit im Rahmen von genehmigten Prüfungshandlungen erfolgen. Der jeweilige Betriebsrat ist auf Anfrage über Prüfungsumfang- und Inhalt zu informieren. Wenn überbetriebliches Recht die Weitergabe von Daten erzwingt und eine vorherige Zustimmung des Betriebsrats nicht möglich ist, wird der Betriebsrat unverzüglich über die übermittelten Daten, die Stelle, die die Daten empfangen hat und den Grund der Übermittlung informiert. Technische Einrichtungen werden nicht [vom Unternehmen] eingesetzt oder genutzt, um Auskunft über den Aufenthaltsort von Beschäftigten zu

erhalten. Ausgenommen ist die Nutzung von IT-Systemen im Rahmen von Geschäftsreisen zur und im Fall von Gefahren für den Mitarbeiter.
Daten, die die Tätigkeit des Konzernbetriebsrates und der lokalen Betriebsräte betreffen, dürfen von keinem anderen Nutzer außer den Mitgliedern der Gremien eingesehen werden. Zu diesem Zweck werden auf den Servern, auf denen diese Daten gespeichert sind, Verzeichnisse eingerichtet, auf die allein Mitglieder der jeweiligen Gremien zugreifen können.
Die vorgenannten Verpflichtungen über Datensicherheit, Weitergabe von Daten sowie [über die] Verarbeitung von Daten gelten in gleichem Umfang, für die Daten, die ausschließlich vom Konzernbetriebsrat und den lokalen Betriebsräten verwaltet werden. Der KBR und die örtlichen BR führen entsprechende Verzeichnisse von Verarbeitungstätigkeiten. Alle freigestellten Betriebsratsmitglieder sind über das Datenschutzgesetz und dessen Anwendung zu schulen. Konzernbetriebsratsmitglieder und lokale Betriebsräte sind kraft ihres Amtes gem. § 79 BetrVG in Bezug auf gekennzeichnete Themen und personenbezogene Daten zur Geheimhaltungspflicht angehalten. Betriebsratsvorsitzende und freigestellte Betriebsräte, die einen begrenzten Zugriff auf das SAP HR System haben, unterschreiben eine Vertraulichkeitserklärung (Anhang 3).

8. Beweisverwertungsverbot

Informationen und Daten, welche die Leistung und/oder Verhalten von Mitarbeitern beschreiben, die unter Verletzung gesetzlicher Vorschriften oder der vorliegenden Betriebsvereinbarung vom Arbeitgeber rechtswidrig gewonnen wurden, dürfen nicht zu Lasten der im Betrieb beschäftigten Arbeitnehmer zu arbeitsrechtlichen Maßnahmen genutzt werden. Die arbeitsrechtlichen Maßnahmen sind rückgängig zu machen. Sowohl der Betriebsrat als auch jeder betroffene Arbeitnehmer können die Löschung dieser Daten und Informationen verlangen. Im Zweifelsfall liegt die Beweispflicht dafür, dass die Informationen oder Erkenntnisse nicht missbräuchlich gewonnen wurden, [beim Unternehmen].

9. Umgang mit Unternehmensdaten und Berechtigungen

Werden Daten an Dritte weitergegeben, so ist vom Unternehmen zu gewährleisten, dass die jeweils gültige […] Vertraulichkeitserklärung [des Unternehmens] eingehalten wird.
Jeder Mitarbeiter erhält im Rahmen seines Tätigkeitsfeldes Zugangsberechtigungen zu Unternehmensdaten. Er darf nicht versuchen, sich auf welchem Wege auch immer, Zugang zu Unternehmensdaten zu verschaffen, für die er keine zugeteilte Zugangsberechtigung hat. Sollte der Mitarbeiter feststellen, dass er Zugang zu mehr Daten als notwendig hat, muss er dieses der zuständigen Administration melden, damit diese den Zugang entsprechend begrenzt.
Berechtigungen zur Einsicht und Bearbeitung von Mitarbeiterdaten werden immer gemäß dem Großvaterprinzip und im Zusammenhang mit der

funktionalen Rolle vergeben. Der Zugriff auf Mitarbeiterdaten für spezielle Unternehmensfunktionen muss zusätzlich vom Country HR Director genehmigt werden.

Mit dem „Großvaterprinzip“ wird auf mehrstufige Berichtslinien in der hierarchischen Unternehmensorganisation Bezug genommen. Der unmittelbare Vorgesetzte – der „Vater“ – eines Beschäftigten darf und muss zur Ausübung seiner Aufgaben auf dessen Daten zugreifen können. Für eine Reihe von Aufgaben ist die Kenntnisnahme und Zustimmung des nächsthöheren Vorgesetzten – des „Großvaters“ – notwendig. Eine Zugriffsberechtigung des Vorgesetzten des Vorgesetzten ist gemäß dieser Regelung zulässig, nicht aber die des „Urgroßvaters“ und freilich ebenso wenig der Zugriff durch „Onkel“ oder „Tanten“, also von Personen aus einer anderen Berichtslinie – eine häufige Begehrlichkeit, z. B. aus dem Marketing mit Zugriffswünschen bezüglich Vertriebsdaten. Die Umsetzung dieser Regelung muss in den einzelnen Systemen, z. B. in Workday oder im CRM Vertriebssystem, durch die Einstellungen des Berechtigungssystems erfolgen und kann technisch sehr aufwendig sein.

Werden Daten auf Servern außerhalb der […] Systeme [des Unternehmens] gespeichert, ist seitens des Unternehmens darauf zu achten, dass die notwendigen Datenschutzmaßnahmen entsprechend der nationalen und EU-Gesetze eingehalten werden. Wann immer möglich, werden Server innerhalb Europas und Ländern mit vergleichbarem Datenschutzniveau bevorzugt. Ist dies nicht möglich, werden auch hier entsprechende Verträge mit den Dienstleistern getroffen, um den EU-Datenschutz zu gewährleisten.

10. Rechte und Pflichten des Betriebsrats

Der Betriebsrat hat die Aufgabe, bereits vorhandene technische Einrichtungen und solche Einrichtungen, deren Einführung für die Zukunft geplant ist, unter dem Aspekt der Möglichkeit der Arbeitnehmerüberwachung zu beurteilen und ggfls. zu reagieren. Auf Verlangen des jeweils zuständigen lokalen Betriebsrats oder Konzernbetriebsrats kann jede vorhandene technische Einrichtung auf Basis dieser Rahmenvereinbarung geprüft werden.

11. Unterrichtung des Betriebsrats

Zur Gewährleistung der Einhaltung dieser Konzernbetriebsvereinbarung wird der Konzernbetriebsrat von der Geschäftsführung rechtzeitig und umfassend über alle Entwicklungen informiert, damit dieser seine gesetzlichen Aufgaben wahrnehmen kann.

Die Information hat umfassend im Rahmen der Projektplanung anhand der Checkliste (Anlage 2) [...] zu erfolgen. Die Checkliste wird seitens Geschäftsleitung und Konzernbetriebsrat archiviert.
Der Konzernbetriebsrat oder der jeweils zuständige lokale Betriebsrat und die Geschäftsführung entscheiden, ob neue technische Einrichtungen auf Basis dieser Rahmenvereinbarung geregelt sind oder eine ergänzende Vereinbarung getroffen werden muss.

Mit der Verankerung des Checklistenverfahrens in dem IT-Projektmanagementsystem werden zwei wesentliche Voraussetzungen für eine effiziente Wahrnehmung der Mitbestimmung gewährleistet: zum einen die „rechtzeitige“, zum anderen die „umfassende“ Information des EDV-Ausschusses. Rechtzeitig, weil immer klar ist, in welchem Projektstadium die Checkliste ausgefüllt werden muss; umfassend, weil die Checkliste selbst diejenigen Informationen, die für den Betriebsrat relevant sind, vollständig abbildet.

Neue technische, lokale oder zentrale Einrichtungen, die persönliche Daten verarbeiten, dürfen erst dann in Betrieb genommen werden, wenn der Konzernbetriebsrat oder der jeweils zuständige lokale Betriebsrat der Inbetriebnahme nach Beratung und ausführlicher rechtzeitiger Information seitens [des] Arbeitgeber[s] zustimmt.
Die neue technische Einrichtung muss immer im Verzeichnis von Verarbeitungstätigkeiten auf Basis der ausgefüllten Checkliste (Anlage 2) gemäß dieser Konzernbetriebsvereinbarung erfasst werden.

12. Prüfungsrechte des Betriebsrats

Der Betriebsrat hat das Recht, alle technischen Einrichtungen, die personenbezogene Daten speichern oder verarbeiten oder die geeignet sind, Informationen über das Verhalten oder die Leistung von Beschäftigten zu generieren, jederzeit kurzfristig mit voll umfänglichen Rechten zu prüfen, um die Funktion und die Einhaltung dieser Betriebsvereinbarung zu überprüfen.
[Das Unternehmen] ist gegenüber dem Betriebsrat zu Auskünften über den Datenschutz und die technischen Einrichtungen zur Arbeitnehmerüberwachung auf Grundlage des Betriebsverfassungsgesetzes jederzeit verpflichtet.
Der Betriebsrat erhält die Möglichkeit, bei Bedarf einen Sachverständigen hinzuzuziehen, der ihn bei der Beurteilung und Kontrolle der Einhaltung dieser Betriebsvereinbarung und seinen sonstigen gesetzlichen Aufgaben im Zusammenhang mit dem Datenschutz und technischen Einrichtungen unterstützt. Hierbei finden die Bestimmungen des § 80 BetrVG Beachtung.

13. Qualifizierungsmaßnahmen für Betriebsratsmitglieder

Betriebsratsmitglieder müssen in der Lage sein, IT-Systeme im Hinblick auf ihren Verwendungszweck und ihre Funktionen im Arbeitsablauf des Betriebs zu beurteilen. Dieses Wissen soll durch Informationen der Geschäftsleitung, IT-Experten und betrieblichen Schulungsmaßnahmen vermittelt werden. Externe Schulungsmaßnahmen im Sinne des § 37 Abs. 6 und 7 BetrVG bleiben hiervon unberührt.

14. Schlussbestimmungen

[…]

Anlage 2 Checkliste
[…]“

Anlage 2 Checkliste

Checkliste: Kriterienraster zur Bewertung von IT-Maßnahmen
Criteria grid for the evaluation of IT measures

Ansprechpartner *Contact:*
Datum *Date:*

1. **Beschreibung des zu implementierenden IT-Systems**
   Description of IT System to be implemented
   1.1 Name des Systems oder Prozesses *Name of the system or process:*
   1.2 Hersteller *Manufacturer:*
   1.3 Überblick über die Hardware/Software, Prozesse und Schnittstellen zu anderen Systemen (z. B. Netzwerkplan, Serverstruktur, Datenbanken, externe Schnittstellen, ggfls. Anlage)
   Overview of hardware/software, processes and interfaces to other systems (i. e. network diagram, server structure, data bases, external interfaces, if necessary provide description)

2. **Zweck der Systemeinführung/des Systembetriebs**
   Purpose of system implementation/system operation
   2.1 Was tut das System?
   What does the system do?

3. **Sieht das IT-System eine Speicherung von Mitarbeiterdaten vor?**
   Does the system include the storage of employee data?

☐ Ja, für Zweck erforderlich *Yes, necessary for the purpose*	☐ Nein *No*	☐ Ja, aber Arbeitgeber verpflichtet sich, gespeicherte Daten nicht zu nutzen (Verweis zu Mustererklärung, die Arbeitgeber abzugeben hat) *Yes, but the employer refrains from using stored data. (Reference to the declaration that employers must submit)*

4. **Welche Mitarbeiterdaten werden gespeichert?**
   Which employee data will be stored?

Nr. ***No.***	**Datum** ***Date***	**Beschreibung** ***Description***	**Ja** ***Yes***	**Nein** ***No***
1	Name, Vorname *Last name, First name*		☐	☐
2	Adressdaten *Address*		☐	☐
3	Geburtsdatum *Date of birth*		☐	☐
4	Familienstand *Marital status*		☐	☐
5	Personalnummer *Personnel number*		☐	☐
6	Staatszugehörigkeit *Citizenship*		☐	☐
7	Renten- und Sozialversicherungsdaten *Pension and social insurance data*		☐	☐
8	Zeiterfassungsdaten (Anwesenheit, Fehlzeiten, Urlaub) *Working Hour Data (Presence, Absence, Vacation)*		☐	☐
9	Qualifikationen *Qualification*		☐	☐
10	Lohn- und Gehaltsdaten *Salary data*		☐	☐
11	Leistungsmerkmale *Employee performance*		☐	☐
12	Bewertung der Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, seiner Leistung und seines Verhaltens *Employee assessment, including his or her abilities, performance and behavior*		☐	☐

5. **Betroffene Bereiche** (Standorte, Arbeitsbereiche, Abteilungen, Mitarbeitergruppen)
   Affected areas *(Locations, Working areas, Departments, Employee groups)*
   5.1 Direkte Anwender (Wer? Wie?) *Users (Who? How?):*
   5.2 IT (z. B. Einführung, Support *i. e. Implementation, Support)* (Wer? Wie? *Who? How?):*
   5.3 Auswirkungen auf andere Bereiche? (Wer? Wie?) *Impact on other areas (Who? How?):*

6. **Wie lange werden die Daten gespeichert?**
   How long is the data stored?

7. **Wo werden die Daten gespeichert?**
   Where is the data stored? (Hoster/Provider)

8. **Liegt eine technische und organisatorische Maßnahme gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g.) und Auftragsverarbeiter (TOM) vor?**
   Technical and organizational measures in accordance with Art. 32 para. 1 DSGVO for persons responsible (Art. 30 para. 1 lit. g.) and order processors (TOM) available?

☐ Ja *Yes* ☐ Nein *No*

9. Wurde der Datenschutzbeauftragte involviert?
Has the Data Protection Officer been involved?

☐ Ja *Yes* ☐ Nein *No*

9.1 Wurde eine Vorabkontrolle durchgeführt? *Has a preliminary check been carried out?*

☐ Ja *Yes* ☐ Nein *No*

9.2 Aufnahme in das Verfahrensverzeichnis erfolgt? *Has it been included in the procedural register?*

☐ Ja *Yes* ☐ Nein *No*

10. Wo werden die Daten geographisch gespeichert?
Where is the data stored geographically?

☐ EU *EU* ☐ Nicht-EU (Drittländer) *Non-EU (3rd countries)*

Wenn Nicht-EU, welches Land? *If non-EU, which country?*

11. Verarbeitung von personenbezogenen Daten im System
Processing of personal data in the system

11.1 Werden Mitarbeiterdaten (z. B. Name oder Benutzerkennzeichen) ausschließlich zum Systembetrieb (Anmeldung, Berechtigungsprüfung) oder zur Kommunikation mit dem Arbeitnehmer (etwa für Rückfragen von Kollegen) genutzt?
Is employee data (e. g. name or user ID) used exclusively for system operation (login, authorization check) or for communication with the employee (e. g. for queries from colleagues)?

Angemeldeter Systembenutzer
Registered system user

☐ Ja *Yes* ☐ Nein *No*

Sonstige Mitarbeiter
Other employees

☐ Ja *Yes* ☐ Nein *No*

11.2 Werden weitere Mitarbeiterdaten als die für den beschriebenen Zweck ausgewertet? *Will any other employee data be evaluated other than for the decsribed purpose?*

Angemeldeter Systembenutzer
Registered system user

☐ Ja *Yes* ☐ Nein *No* ☐ anonymisiert* *anonymized*

Sonstige Mitarbeiter
Other employees

☐ Ja *Yes* ☐ Nein *No* ☐ anonymisiert* *anonymized*

*anonymisiert/aggregiert: Der einzelne Mitarbeiter lässt sich nicht mehr bestimmen, beispielsweise weil die Daten von mehr als sechs Beschäftigten zusammengefasst wurden.
**anonymized/aggregated: The individual employee can no longer be determined, for example, because the data of more than six employees has been combined.*

Wenn Ja, im Anhang aufzählen: welche Daten, zu welchem Zweck, Liste der Berichte
***If yes, please describe (attachment)**: which data, for which purpose, attach list of reports or description*

Welche Auswertungen finden statt? Liste der Berichte oder Beschreibung im Anhang
***Which evaluations/reports are generated?** Attach list of reports or description*

Sonstige Bemerkungen
Other comments

12. Projektzeitplan
Project Time Plan
Information bei Ausgang Tollgate 1, spätestens Eingang Tollgate 2
Information Tollgate 1, latest start Tollgate 2

Optional Projektplan im Anhang- ergänzend zu Punkt 11.1–11.5 nachfolgend
Optional add project time plan supplementing points 11.1–11.5 ff.

12.1 Beginn/Ende Planungszeitraum *Start/End Planning period:*
12.2 Beginn/Ende IT-Realisierung und Tests *Start/End of IT implementation and testing:*
12.3 Beginn/Ende Schulungen *Start/End of Training(s):*
12.4 Beginn/Ende Piloteinführung *Start/End of pilot introduction:*
12.5 Beginn/Ende Echtzeitbetrieb (Einsatz) *Start/End of real time implementation:*

13. Geplante Übermittlung von Beschäftigtendaten in andere interne Systeme
Planned data transfer of employee data in other internal systems

☐ Ja *Yes* ☐ Nein *No* – wenn Ja *if yes:*

Welche Daten? *Which data?*
In welche Systeme? *In which systems?*
Zu welchem Zweck? *For which purpose?*

14. Geplante Übermittlung von Beschäftigtendaten außerhalb [des Unternehmens]/BSN:
Planned transfer of employee data outside of [the company]/BSN
☐ Ja *Yes* ☐ Nein *No* – wenn Ja *if yes*:

Empfänger *Recipient:*
Zu welchem Zweck? *For which purpose?*

Wenn Ja:
If yes:
☐ Es liegt eine Auftragsdatenverarbeitung nach Art. 28 ff. EU-DSGVO vor.
☐ Die Datenverarbeitung erfolgt im Rahmen einer Funktionsübertragung.
☐ Die Datenverarbeitung/-weitergabe erfolgt in einem Land außerhalb der EU.
☐ *It is considered order data processing according to* Art. 28 ff. EU-DSGVO
☐ *The data processing is performed in the context of a transfer function.*
☐ *The data processing/data transfer takes place in a country outside of the EU.*

Bei Änderungen von einzelnen Punkten dieser IT-Maßnahme ist eine neue Bewertung vorzunehmen!
In case of any changes of the individual points of this IT measure, a new evaluation must be carried out!

Kriterienraster genehmigt durch:

Datum:
Projekt/IT-Leitung
Arbeitsdirektor/HR Direktor
Datenschutzbeauftragte/r
Ergebnis der Bewertung (wird von der Belegschaftsvertretung ausgefüllt!):

☐ Keine Regelung notwendig, Systemeinsatz wie beschrieben freigegeben; die Checkliste wird im Zusammenhang mit der IT-Rahmenvereinbarung von Geschäftsführung und Konzernbetriebsrat archiviert.
☐ Weiterer Informations- und Beratungsbedarf
☐ Regelung notwendig:
  ☐ Protokollnotiz (legt konkrete Absprachen/Rahmenbedingungen fest, z. B. für den Pilotbetrieb)
  ☐ Betriebsvereinbarung

Datum:

KBR-Vorsitzender	**KBR-EDV-Ausschuss-Sprecher**

Quelle der Vereinbarungen: Die Kennung am Ende des Zitats bezeichnet die thematische Zuordnung, das Jahr des Abschlusses und den Standort im Archiv Betriebliche Vereinbarungen.

Ihr seid die Experten – schickt uns eure Vereinbarungen und profitiert voneinander!

Habt ihr eine gute Vereinbarung zum Thema Digitalisierung abgeschlossen? Wir interessieren uns für die Geschichte und Fakten dahinter und freuen uns über eure Zusendung, elektronisch oder per Post. Wir werten sie aus und stellen euer wertvolles Wissen allgemein zur Verfügung – vertraulich, anonym und als Beitrag für eine mitbestimmte Arbeitswelt der Zukunft.

Macht mit und nehmt mit uns Kontakt auf!

www.boeckler.de/betriebsvereinbarungen

Mitbestimmungsportal

Der Böckler-Infoservice bietet Mitbestimmungsakteurinnen und -akteuren spezifisches Handlungs- und Orientierungswissen, u. a. Branchenmonitore, Themenradar, Wissen kompakt, Szenarien „Mitbestimmung 2035".

Jetzt kostenlos anmelden auf:

www.mitbestimmung.de