



Musterbetriebsvereinbarung zur Implementierung von Industrie 4.0 – Anwendungen

Datum: 20.02.2018

Autoren: Prof. Dr. Gerrit Hornung

Wiss. Mitarbeiter Helmut Lurtz

1 Eckpunkte für eine Betriebsvereinbarung über die Einführung und Anwendung technischer Einrichtungen

Die Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, ist nach § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig. Der Rechtsprechung genügt die objektive Eignung zur Überwachung (ständige Rechtsprechung seit BAGE 27, 256), weshalb die Einführung von Arbeitsplatzassistenzsystemen oder anderen Verfahren, die auf eine Profilbildung angelegt sind, regelmäßig der Mitbestimmung unterfallen wird. Neue technische Möglichkeiten der Industrie 4.0 bieten – etwa durch moderne IT als Arbeitsmittel – einerseits eine Entlastung der Beschäftigten, andererseits stellt sich die Frage, ob diese als potenzielle Mittel der Überwachung die Rechte und Interessen der Beschäftigten beeinträchtigen. In Zeiten der Digitalisierung und von Big Data-Analysen wird fast alles gemessen, gespeichert und ausgewertet. So können Beschäftigte nunmehr viel einfacher nach der Intensität der Nutzung von Systemen bewertet werden. Je weiter also die Digitalisierung im Arbeitsverhältnis voranschreitet, desto größere Bedeutung erlangt das erzwingbare Mitbestimmungsrecht des Betriebsrates nach § 87 Abs. 1 Nr. 6 BetrVG.

Folgende Eckpunkte – basierend auf den Eckpunkten von *P. Wedde*, Handbuch Datenschutz und Mitbestimmung, S. 237ff.¹ – sollen als Leitfaden für Betriebsvereinbarungen zur Einführung und Anwendung technischer Einrichtungen dienen. Diese Liste erhebt keinen Anspruch auf Vollständigkeit, insbesondere vor dem Hintergrund der sich ständig ändernden Technik und verschiedenen Einzelfällen im IT-Bereich. Sie soll vielmehr als Anhaltspunkt und Orientierungshilfe in Form einer Checkliste für Betriebsvereinbarungen insbesondere im IT-Bereich dienen.

Zweckbestimmung	Den Zweck der erhobenen oder sonst erlangten Daten genau festlegen und vereinbaren, dass diese nur zu diesem Zweck verarbeitet werden dürfen (Zweckbindung); keine Zweckentfremdung erhobener oder verarbeiteter personenbezogener Daten
Verfolgte Ziele	<p>Aus Arbeitgebersicht könnten diese in etwa sein:</p> <ul style="list-style-type: none"> • Schutz der Betriebsmittel • (Gerechte) Verteilung der Arbeit • Kontrolle der Arbeitszeit • Qualitätssicherung und deren Kontrolle • Effizienzsteigerung • Ungehinderte Umsetzung unternehmerischer Investitionsentscheidungen • Verbesserung der Arbeitsabläufe • Prozessoptimierung • Untersuchung von Compliance-Verstößen • Auslastungsanalysen <p>Aus Beschäftigtensicht könnten diese in etwa sein:</p> <ul style="list-style-type: none"> • Ausschluss der Überwachung • Berücksichtigung der Benutzerfreundlichkeit

¹ Wedde 2016, S. 237ff. Rn. 231ff.

	<ul style="list-style-type: none"> • Berücksichtigung des Gesundheitsschutzes: Anwendung der arbeitswissenschaftlichen Erkenntnisse zum Arbeits- und Gesundheitsschutz, Ergonomie • Zusammenwirken Mensch-Arbeitsmittel bzw. Mensch-Maschine • Schutz vor Rationalisierung, Arbeitsplatzsicherung • Einsatz nur zur Erleichterung der Arbeit
Kategorien der erfassten Daten	<ul style="list-style-type: none"> • Eine detaillierte Darstellung der einzelnen erfassten Daten ist nicht zuletzt aufgrund ihrer Komplexität meistens nicht ratsam. Durch einfache Updates der Software können einfach Änderungen vorgenommen werden, die die in der Betriebsvereinbarung festgelegte Erfassung obsolet werden lassen. Vielmehr sollte eine genaue Darstellung der Auswertungen erfolgen, die wiederum bestimmte Datenkategorien festlegen kann. • Besonders strenge Regeln gelten nach Art. 9 DSGVO für sensible Daten wie etwa die ethnische Herkunft oder genetische und biometrische Daten.
Erlaubnistatbestand	<p>Sofern die Verarbeitung von personenbezogenen Daten auf die Betriebsvereinbarung als Erlaubnistatbestand gestützt werden soll, so muss dies aus dem Wortlaut der Vereinbarung klar hervorgehen.</p>
Hinweis auf datenschutzrechtlichen Grundsätze	<p>Die geregelte Datenverarbeitung muss sich innerhalb der durch die allgemeinen Grundsätze der DSGVO gesteckten Grenzen halten (Art. 5 Abs. 1 lit. a bis f DSGVO). Betriebsvereinbarungen sollten einen Hinweis hierauf enthalten.</p>
Hard- und Softwarebeschreibung	<ul style="list-style-type: none"> • Welches System soll genutzt werden (z.B. Sharepoint) • Welche Version (Versionsnummer und Datum) kommt zum Einsatz; alternativ bei Software as Service: welcher Stand besteht bei der Einführung • Welche Hardware (z.B. Dome-Kameras mit 360°-Drehung, Drohnen) soll genutzt werden • Datenschutz von Anfang an mitbedacht: „Datenschutz by Design“ (entsprechende Information an den Betriebsrat zu Beginn des Mitbestimmungsverfahrens) • Schnittstellen zu anderen Systemen und Datenflüsse abschließend und vollständig festlegen
Datenschutzbeauftragter	<ul style="list-style-type: none"> • Grds. ist die Einbindung stets vorteilhaft, in vielen Fällen aber auch rechtlich verbindlich • Stellungnahme muss zu jedem einzuführenden IT-System beigefügt werden; ggf. Einladung zur BR-Sitzung (Art. 38 Abs. 1 DSGVO) • Damit der Datenschutzbeauftragte seine Beratungspflicht aus Art. 39 Abs. 1 lit. a DSGVO erfüllen kann, ist ihm Zugang zu allen erforderlichen Informationsquellen zu ermöglichen (Art. 38 Abs. 2 DSGVO)

	<ul style="list-style-type: none"> • Regelmäßige (z.B. vierteljährliche) Einladung zu Betriebsrats-sitzungen, auch zum Bericht über die Anwendung und ggf. Fortschreibung der Betriebsvereinbarung • Tätigkeitsbericht; auch an den Betriebsrat
Einsatzort	<ul style="list-style-type: none"> • Möglichst exakte Beschreibung (Transparenz für die Beschäftigten) • Möglichst eingeschränkt, wenn Überwachung möglich ist
Einsatzzeit und Umfang	<ul style="list-style-type: none"> • Möglichst exakte Beschreibung • Auf das datenschutzrechtlich Erforderliche beschränken • Bei vielen technischen Systemen richtet sich das nach den betrieblichen Erfordernissen • Bei Systemen, die gezielt die Kontrolle von Beschäftigten bezwecken, ist als Grundsatz nur eine anlassbezogene Kontrolle zulässig
Auswertungen	<p>Welche Auswertungen sind vorgesehen?</p> <ul style="list-style-type: none"> • <u>Leistungs- und Verhaltenskontroll-Auswertungen (LVK)</u>: Verhaltens- und Leistungskontrolle ist durch den Arbeitgeber gerade bezweckt; disziplinarische oder arbeitsrechtliche Maßnahmen aufgrund dieser Daten sind möglich. Die Betriebsparteien können hierbei die Art und die Voraussetzungen von Disziplinarmaßnahmen festlegen. So kann vereinbart werden, dass erst nach einer bestimmten Anzahl an wiederholter „Fehlleistungen“ ein abmahnungsfähiger Tatbestand vorläge. • <u>Reine Informations-Auswertungen</u>: keine Verhalten- und Leistungskontrollen bezweckt; dient lediglich der Information des Arbeitgebers über bspw. die Auswertung der Fehlermeldungen einer bestimmten Maschine zum Zweck einer vorausschauenden Instandhaltung. Die Grenze von Info-Auswertungen und LVK-Auswertungen ist fließend und unterliegt in einem gewissen Maße den Verhandlungen der Betriebsparteien. Je mehr sich eine Auswertung zur Überwachung des Verhaltens des Beschäftigten eignet, umso eher ist diese als LVK-Auswertung zu werten. • <u>Aggregierte Auswertungen</u> sind zwar grundsätzlich nicht personenbezogen. Es sollte jedoch festgelegt werden, in welchen Fällen tatsächlich eine aggregierte Auswertung vorliegen soll. So könnte eine Auswertung, die nur die Fehlerquote aller über 55-jährigen in einer bestimmten Produktionsgruppe anzeigt, trotz Kulminierung einer Vielzahl von Daten, einzelne Personen zu erkennen geben.
Ausnahmekatalog zu ausdrücklich erlaubten Auswertungen	<ul style="list-style-type: none"> • Denkbar ist ein Ausnahmekatalog zu zulässigen Auswertungen (können auch das Verhalten bzw. die Leistung erfassen) • Die Inhalte von Arbeitsergebnissen an sich • Missbrauchsfälle: sofern ein dringender Tatverdacht auf eine schwere Pflichtverletzung sowie Straftaten oder Ordnungswidrigkeiten des AN vorliegt. An dieser Stelle wird vereinzelt

	<p>versucht, einen Zustimmungsvorbehalt des Betriebsrats zu implementieren.</p> <ul style="list-style-type: none"> • Zunächst nur anonymisiert möglich; im Fall von Bagatellen findet keine weitere Auswertung statt • Personenbezogen nur begrenzt: nur soweit Datensicherheit und Datenschutz das gebieten (z.B. Eingabekontrolle) <p>Personenbezogen allenfalls, wenn ein durch dokumentierte tatsächliche Anhaltspunkte begründeter konkreter Verdacht einer Straftat besteht und nur mit Zustimmung und im Beisein des Betriebsrates; Vorstufe sollte ein Gespräch mit dem Betroffenen im Beisein des Betriebsrates sein.</p>
Zugriffsberechtigungen	<ul style="list-style-type: none"> • Möglichst eng regeln • Je granulierter personenbezogene Daten sind, desto weniger Personen (insbesondere die Personalabteilung) sollten Zugriff auf diese haben. • LVK-Auswertungen sollen auf die nötigsten Personen/Abteilungen beschränkt werden. Aggregierte Auswertungen hingegen können weitflächiger zugänglich sein. • Beschäftigte selber sollen stets berechtigt sein, ihre personenbezogenen Daten einzusehen
Privatnutzung	Möglichst klar regeln, z.B. bei Internet und Email, dienstlichem Laptop, BYOD, etc.
Rollen- und Berechtigungskonzepte	<ul style="list-style-type: none"> • Vollständig und abschließend regeln • Technische Schutzmaßnahmen festlegen
Rechte Betroffener	<ul style="list-style-type: none"> • Einbeziehung Betroffener (z.B. durch Digitalisierung oder Automatisierung) in Projekte und Arbeitsgruppen • Technisch-organisatorische Voraussetzung für Umsetzung der Betroffenenrechte festlegen (v.a. Auskunfts- und Berichtigungsansprüche)
Rechte des Betriebsrats	<ul style="list-style-type: none"> • Jede Einführung, Ergänzung und Änderung ist mitbestimmungspflichtig • Bestimmung welche Unterlagen vorzulegen sind: z.B. Systemdokumentation in verständlicher Form inkl. Stellungnahme des Datenschutzbeauftragten • Hinzuziehung externer Sachverständiger nach freier Wahl möglich • Auswertungen sind mitbestimmungspflichtig, Regelauswertungen ggf. in der Anlage hinterlegen • Kontrolle der Einhaltung jederzeit möglich • Zuständige sind auskunftspflichtig • Qualifizierung für das gesamte Gremium
Erhöhung der Transparenz	Konkretisierungen der Transparenzpflichten aus Art. 12-22, 34 DSGVO, wie etwa Auskunftsformate oder -verfahren

Sanktion	<ul style="list-style-type: none"> • Ein Beweisverwertungsverbot für personenbezogene Daten und Erkenntnisse, die unter Verstoß gegen die Bestimmungen der Betriebsvereinbarung erfolgen, sollte vereinbart werden. • bei Verstößen gegen die Betriebsvereinbarung: umgehende Abschaltung des Systems • Unterlassungsanspruch: z.B. zur Abschaltung bestimmter Systemteile • Heranziehung externen Sachverständigen
Qualifizierung	<p>Qualifizierungskonzepte für Beschäftigte (z.B. Lernziele, Kerninhalte, Teilnehmer, Termine und Orte der Bildungsmaßnahmen) sind stets zu regeln</p>
Löschung	<ul style="list-style-type: none"> • Möglichst frühzeitig (Grundsatz der Datenminimierung) • Prüffristen festlegen • Allgemeines Lösungskonzept und technisch sichere Lösungsmechanismen definieren
Speicherort	<ul style="list-style-type: none"> • Land und Gesellschaft festlegen • Grds. Speicherung in der EU; bei (z.B. konzernweiten) Speicherungen in Drittländern Beachtung der Art. 44 ff. DSGVO (Speicherung dort grds. nur bei angemessenem Datenschutzniveau bzw. alternativer Garantien) • Im Falle einer Auftragsdatenverarbeitung, sind die Voraussetzungen der Art. 28 ff. DSGVO zu beachten.

2 Musterbetriebsvereinbarung zur Einführung von IT-Systemen auf der Grundlage des § 87 Abs. 1 Nr. 6 BetrVG

Betriebsvereinbarungen als flexible und sehr individuelle Werkzeuge des Betriebsrates können ihre legitimierende sowie regelnde Wirkung nur entfalten, wenn sie den jeweiligen Sachverhalt in vollem Umfang erfassen und auf den Einzelfall maßgeschneidert sind. Musterbetriebsvereinbarungen können diesem Zweck selten gerecht werden, da sie meist sehr generisch und ohne Änderungen und Ergänzungen wenig praxistauglich sind. Aus diesem Grund ist die im Folgenden aufgeführte Musterbetriebsvereinbarung (basierend auf Holthaus, M. 4. Muster: Einführung, Einsatz und Weiterentwicklung von DV-/IT-Systemen in: Hümmerich, K./ Lücke, O./ Mauer, R., Arbeitsrecht – Vertragsgestaltung. Prozessführung, Personalarbeit, Betriebsvereinbarungen, 9.Auflage, 2018, § 5, Rn. 132.) nur als Ausgangspunkt für konkretere Betriebsvereinbarungen zu gebrauchen und muss den einzelnen Umständen angepasst bzw. ergänzt oder ganz verändert werden. Ein universelles Muster, das Gültigkeit für verschiedene Szenarien erhebt, kann aufgrund der genannten Probleme nicht konstruiert werden. Deshalb wird exemplarisch eine möglichst offen gestaltete Musterbetriebsvereinbarung bereitgestellt, die die Verarbeitung von personenbezogenen Daten in IT-Systemen regeln soll.

Zwischen

Firma _____

gesetzlich vertreten durch _____ (nachfolgend „Gesellschaft“ genannt)

und

Betriebsrat des Betriebs der Firma _____ (nachfolgend „Betriebsrat“ genannt)

wird gemäß § 87 Abs. 1 Nr. 6 BetrVG² folgende Betriebsvereinbarung über die „Einführung von IT-Systemen“ geschlossen:

Präambel³

Die Gesellschaft und der Betriebsrat legen mit dieser Betriebsvereinbarung Rahmenbedingungen für den Einsatz von [IT-Systemen] mit dem Ziel fest, die Persönlichkeitsrechte der Beschäftigten unter Beachtung aller maßgeblichen rechtlichen Vorgaben zu wahren und zu sichern. Folgende betriebliche Regeln werden auf der Grundlage gegenseitigen Vertrauens gebildet, um den Interessen beider Seiten gerecht werden. Vor dem Hintergrund der Datenschutz-

² Sofern die Verarbeitung von personenbezogenen Daten auf die Betriebsvereinbarung als Erlaubnistatbestand gestützt werden soll, so muss dies aus dem Wortlaut der Vereinbarung klar hervorgehen. Eine explizite Erwähnung in der Präambel oder den Begriffsbestimmungen ist ebenfalls denkbar.

³ Zusammenfassung des Zwecks der Betriebsvereinbarung.

Grundverordnung, des neuen Bundesdatenschutzgesetzes und des Betriebsverfassungsgesetzes sowie der EU-Richtlinien und weiterer Gesundheits- und Arbeitsschutzbestimmungen wird folgende Vereinbarung geschlossen.

§ 1 Begriffsbestimmungen⁴

(1) Personenbezogene Daten sind i.S.d. Art. 1 lit. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

(2) Verarbeiten ist i.S.d. Art. 1 lit. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(3) Definition der genauen Anwendung [IT-Systeme]: Beschreibung der konkreten Hardware und Software: z.B. Informations- und Techniksysteme sind Hard- und Software. Hierzu gehören sämtlicher Peripheriegeräte, digitale Nebenstellenanlagen, Netze, etc. Projekte sind Vorhaben, die durch die Einmaligkeit der Bedingungen in ihrer Gesamtheit, durch eine Zielvorgabe, die Begrenzung zeitlicher, personeller oder anderer Art, Abgrenzung gegenüber anderen Vorhaben und eine projektspezifische Organisation gekennzeichnet ist.

(4) Weitere Begriffsbestimmungen, die zum Verständnis der Betriebsvereinbarung notwendig sind: z.B. Projektmitglieder sind die einem Projekt zugeordneten Beschäftigte, die nicht mit der Projektleitung oder -koordination oder deren Stellvertretung beauftragt sind.

§ 2 Grundsätze

(1) Die geregelte Datenverarbeitung muss sich innerhalb der durch die allgemeinen Grundsätze der DSGVO gesteckten Grenzen halten. Die Grundsätze der rechtmäßigen Verarbeitung von personenbezogenen Daten der Verarbeitung nach Treu und Glauben, der Transparenz, des Zweckbindungsgrundsatzes, der Datenminimierung, der Datenrichtigkeit, der Speicherbegrenzung, der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 lit. a bis f DSGVO werden beachtet.

(2) Weitere Grundsätze, die für das [IT-System] erforderlich sind wie etwa bei IT-Systemen zur Informations- und Kommunikationstechnologien: „Es gilt der Grundsatz der persönlichen und der nicht-maschinellen Kommunikation.“

⁴ Begriffsbestimmungen sollen alle wichtigen im Vertragstext gebrauchten Begriffe erläutern.

§ 3 Geltungsbereich

(1) Die Betriebsvereinbarung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Sie gilt nicht für Personalinformations- und -verwaltungssysteme. Für diese sind gesonderte Betriebsvereinbarungen abzuschließen.

(2) Die Betriebsvereinbarung erstreckt sich auf alle Beschäftigte des Unternehmens, die unter den Begriff des Arbeitnehmers i.S.d. § 5 Abs. 1 BetrVG fallen. Diese Vereinbarung entfaltet keine Wirkung auf leitende Angestellte gem. § 5 Abs. 3 BetrVG.

(3) Die Betriebsvereinbarung gilt für alle Betriebsteile des Unternehmens. Sie umfasst insbesondere auch Telearbeit außerhalb der Geschäftsräume sowie Außendienstmitarbeiter.

(4) Verträge mit sowie Aufträge an Dritte dürfen dieser Vereinbarung nicht widersprechen und sind so zu gestalten, dass die Kontrollrechte des Betriebsrats auch gegenüber Dritten wahrgenommen werden können.

§ 4 Einsatzzweck und Zweckbindung

(1) Die Gesellschaft setzt [IT-Systeme] bei [Ort und Bereich der Anwendung] ein, die die Beschäftigten zur Ausübung ihrer Tätigkeit nutzen.

(2) [IT-Systeme] werden zur Verbesserung der Arbeitsabläufe [Angabe des konkreten Vorteils, z.B. Organisation des Schichtplans, Optimierung von Wartungsintervallen, Unterstützung bei der Kommissionierung, Bereitstellung visueller Unterstützung bei Arbeitsabläufen, effizientere und gerechtere Verteilung von Schichten, Verbesserung der Auslastung der Maschinen und Beschäftigten] sowie zum Schutz der Betriebsmittel vor Straftaten und anderen Rechtsverstöße eingesetzt (z.B. Schutz vor Diebstählen).

(3) Zudem sollen durch den Einsatz von [IT-Systemen] die Einsätze der Beschäftigten koordiniert werden, die an das Vertriebsmanagement der Gesellschaft angeschlossen sind. Auf diese Weise soll eine beschleunigte Auftragsbearbeitung sowie eine Verbesserung von Kundenbetreuung und Servicequalität erreicht werden.

(4) Der Einsatzzweck ist ausschließlich auf die oben genannten Zwecke begrenzt.

§ 5 Erprobung der [IT-Systeme]

(1) Die Parteien vereinbaren, neue [IT-Systeme] als Arbeitsmittel zunächst in einer Erprobungsphase für die Dauer von [Zeitdauer] einzusetzen. In dieser Phase können die Beschäftigten die Systeme nach einem koordinierten Plan testweise nutzen.

(2) Während dieser Erprobungsphase findet durch eine zu benennende Arbeitsgruppe unter Beteiligung von betroffenen Beschäftigten und Einbeziehung des Datenschutzbeauftragten eine begleitende Überprüfung der Einsatzauswirkungen statt. Der Betriebsrat hat diesbezüglich ein Teilnahme- und umfassendes Informationsrecht.

(3) Die Beschäftigten berichten in der Erprobungsphase über Hindernisse und geben Hinweise an die Arbeitsgruppe für eine bessere Gestaltung des [IT-Systems].

(4) Die Arbeitsgruppe führt eigenständig Untersuchungen und Evaluationen hinsichtlich der Funktionsfähigkeit und weiteren Verbesserungsmöglichkeiten durch. Die Arbeitsgruppe hat diesbezüglich die Einwilligung der Geschäftsleitung.

§ 6 Durchführungsmodalitäten⁵

(1) Es werden nur die Systeme und Systemfunktionen verwendet, die dem Betriebsrat benannt wurden. Im Übrigen gilt § 8.

(2) [Beschreibung der Funktion und des Ablaufs des IT-Systems]

(3) Die Installation bzw. Freischaltung von [IT-Systemen] am einzelnen Arbeitsplatz und damit die Berechtigung der Nutzung sollen erst nach erfolgter Qualifizierung der Beschäftigten geschehen.

(4) Neue und ausscheidende Beschäftigte werden an die Systemadministratoren gemeldet.

(5) In der Anlage [Ziffer der Anlage] der Betriebsvereinbarung sind sämtliche Software und Hardware aufgeführt, die im Rahmen der [IT-Systeme] eingesetzt werden. Weiterhin definiert die Anlage [Ziffer der Anlage] die Datenkategorien sowie Informationen des eingesetzten IT-Systems, auf die im Rahmen der Nutzung des [IT-Systems] zurückgegriffen wird.

§ 7 Verhaltensregeln und Geheimhaltungspflichten

(1) Beschäftigte dürfen Informationen zu personenbezogenen Daten, die sie im Rahmen ihrer Projektarbeit erhalten, keinen Personen außerhalb des Arbeitskreises zugänglich machen. Diese Verpflichtung gilt auch nach Beendigung des Arbeitsverhältnisses.

(2) Die Gesellschaft verpflichtet sich Abs. 1 durch technische und organisatorische Maßnahmen zu gewährleisten.

(3) Der Beschäftigte ist verpflichtet, Geschäfts- und Betriebsgeheimnisse sowie betriebliche Angelegenheiten vertraulicher Natur, die als solche von der Geschäftsleitung schriftlich gekennzeichnet oder mündlich bezeichnet bzw. offensichtlich als solche zu erkennen sind, geheim zu halten und ohne ausdrückliche Genehmigung der Geschäftsleitung keinen dritten Personen zugänglich zu machen.

(4) Betriebs- und Geschäftsgeheimnisse sind Tatsachen, die im Zusammenhang mit einem Geschäftsbetrieb, die nur einem eng begrenzten Personenkreis bekannt sind, nicht offenkundig sind, nach dem bekundeten Willen des Betriebsinhabers geheim gehalten werden sollen und an deren Geheimhaltung der Unternehmer ein berechtigtes Interesse hat.

⁵ Möglichst präzise Beschreibung des eingeführten IT-Systems.

§ 8 Mitbestimmung bei der Einführung weiterer bzw. Erweiterung bestehender [IT-Systeme]

(1) Die Einführung zusätzlicher Systeme, die Schaffung von Schnittstellen zu weiteren IT-Systemen, Zugriffsberechtigungskonzepte, die Verarbeitung und Auswertung personenbezogener Daten, Qualifizierungskonzepte usw. unterliegen der Mitbestimmung des Betriebsrats und sind durch eine weitere Betriebsvereinbarung zu regeln. Die Änderung vorhandener Anwendungen sind mitbestimmungspflichtig, sobald personenbezogene Daten hinzukommen oder neue Auswertungen auf vorhandene personenbezogene Datenfelder vorgenommen werden. Jegliche Maßnahmen zur Einführung, Ergänzung oder Änderung von [IT-Systemen] werden dem Betriebsrat so rechtzeitig bekannt gegeben, dass dieser in der Lage ist Gestaltungsalternativen einzubringen.

(2) Der Betriebsrat ist über die Zwecke der Anwendung, Implementierungsschritte sowie Einbindung des Systems in die bestehende IT-Strategie des Unternehmens zu informieren. Hierbei sind insbesondere die technischen Komponenten und Eigenschaften, Einsatzfelder- sowie Orte anzugeben. Die möglichen Auswirkungen auf die Beschäftigten sind zu erforschen und zu detailliert zu beschreiben.

(3) Der Betriebsrat überprüft vorrangig die Sicherstellung der in § 10 genannten Sachverhalte. Verstoßen Teile des Systems gegen gesetzliche, tarifvertragliche oder betriebliche Bestimmungen, widerspricht der Betriebsrat der Einführung.

(4) Folgende Anlagen werden nach erfolgter Zustimmung des Betriebsrates erstellt:

In [Anlage 1 Hardware-Verzeichnis] werden alle bedeutsamen Hardwarebestandteile und die Netzwerkstruktur beschrieben.

In [Anlage 2 Softwareverzeichnis] werden sämtliche Systeme und Systemfunktionen beschrieben.

In [Anlage 3 Auswertungsverzeichnis] werden alle Auswertungen und Datenaggregationen personenbezogener Daten mit Hilfe von [IT-Systemen], die Verknüpfung von Daten verschiedener Systeme und der Datenexport zur anderweitigen Verarbeitung von Daten und der zugehörigen Vereinbarungen dokumentiert.

In [Anlage 4 Berechtigungsverzeichnis] sind Zugriffsberechtigungskonzepte zu erstellen und zu dokumentieren. Die Systemadministratoren sind zu benennen.

§ 9 Weitere Rechte des Betriebsrats

(1) Der Betriebsrat ist jederzeit zur Kontrolle der Einhaltung der Vereinbarungen der vorliegenden Betriebsvereinbarung sowie der gesetzlichen Vorgaben berechtigt. Hierzu wird der Betriebsrat ermächtigt lesenden Zugriff auf die Systemfunktionen zu nehmen. Die Abteilungen der Systemadministration sowie Anwendungsentwicklung sind dem Betriebsrat zu Auskünften über Systeminhalte und deren Anwendungen verpflichtet. Der Betriebsrat kann den Datenschutzbeauftragten zur Kontrolle hinzuziehen.

(2) Die Gesellschaft informiert den Betriebsrat – unbeschadet der gesetzlichen Mitbestimmung – regelmäßig und umfassend über die laufende IT-Planung.

(3) Der Betriebsrat kann sich im Rahmen der gesetzlichen Aufgaben durch externe Sachverständige nach vorheriger Information der Geschäftsleitung beraten zu lassen. Die entstandenen Kosten werden durch die Gesellschaft getragen.

§ 10 Leistungs- und Verhaltenskontrolle

(1) Eine automatisierte Verarbeitung von Daten zur Leistungs- oder Verhaltenskontrolle, zum Leistungsvergleich oder zur Leistungsbemessung von Beschäftigten ist unzulässig. Ausnahmen bedürfen der ausdrücklichen Vereinbarung mit dem Betriebsrat unter Einbeziehung des Datenschutzbeauftragten.

(2) Im Rahmen des Projektmanagements erfasste Daten und durchgeführte Auswertungen dürfen ausschließlich zur Planung, Zeit- und Kostenkontrolle des Projekts verwendet werden.

(3) Der Betriebsrat ist im Falle von Prüfungen, die aufgrund gesetzlicher oder tariflicher Vorschriften und Verordnungen erforderlich sind, unverzüglich von der entsprechenden Maßnahme in Kenntnis zu setzen. Der Betriebsrat wird über die beabsichtigte Prüfung seitens der mit der Prüfung beauftragten Stelle vollständig informiert und hat das Recht an der Prüfung teilzunehmen.

§ 11 Auswertungen

(1) Daten und Auswertungen in Bezug auf Beschäftigte erfolgen grundsätzlich, soweit nicht gesondert und ausdrücklich geregelt, in anonymisierter Form. Anonymisiert sind Daten und Auswertungen, wenn sie derart verändert sind, dass die Einzelangaben nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einem bestimmten Beschäftigten zugeordnet werden können. Abweichungen von diesem Grundsatz sind nur möglich, sofern die Grundsätze des Datenschutzes gewahrt bleiben.

(2) Für Auswertungen zu Leistungs- und/oder Verhaltenskontrolle gilt § 10.

(3) Liegt ein konkreter Tatverdacht auf eine schwere Pflichtverletzung sowie Straftaten oder Ordnungswidrigkeiten des Beschäftigten vor, kann der Arbeitgeber Auswertungen zur Aufklärung des Verstoßes durchführen. Im Fall von Bagatellen findet keine Auswertung statt.

(4) Aufgrund der Untersuchung nach Absatz 3 ist ein Bericht zu erstellen. Der betroffene Beschäftigte ist so früh wie möglich anzuhören. Hat sich der Verdacht nicht bestätigt, ist der Bericht zu vernichten, es sei denn, der Beschäftigte widerspricht der Vernichtung. Der Betriebsrat ist auf Wunsch des Beschäftigten hinzuzuziehen.

(5) Die Gesellschaft unterlässt es, ohne ausdrückliche Zustimmung des Betriebsrates Auswertungen von personenbezogenen Daten, die durch diese Betriebsvereinbarung ausgeschlossen sind, durch Dritte vornehmen zu lassen bzw. zu verwenden.

(6) Soweit im Einsatz befindliche [IT-Systeme] Aktivitäten der Beschäftigten aufzeichnen, dürfen diese nur:

- zur Gewährleistung der Systemsicherheit,
- zur Gewährleistung von Datenschutz- und Datensicherheit,

- zur Überprüfung der Einhaltung von Betriebsvereinbarungen und gesetzlichen Vorschriften,
- zur Analyse und Korrektur technischer Fehler in den Systemen zur Steuerung und Optimierung der Systeme,
- zur Abrechnung verbrauchter Systemleistungen,
- zur Wahrung gesetzlicher Aufbewahrungspflichten,
- zur Wahrung von Prüfungsaufgaben durch Finanzbehörden und Wirtschaftsprüfer benutzt werden.

§ 12 Zugriffsberechtigungen

- (1) Der Zugriff auf personenbezogene Daten, die dazu geeignet sind das Verhalten oder die Leistung zu kontrollieren ist auf einen möglichst geringen Personenkreis zu beschränken.
- (2) Die Gesellschaft verpflichtet sich die Zugriffsbeschränkung durch geeignete technische und organisatorische Maßnahmen zu gewährleisten.
- (3) Grundsätzlich zugriffsberechtigt sind folgende Personen: [Personen, die zur Erreichung des festgelegten Zwecks auf diese Daten zugreifen müssen, z.B. die dem Betroffenen weisungsberechtigten Vorgesetzten, die Geschäftsführung oder die von dieser hierfür beauftragten Personen, der Betriebsrat]
- (4) Systemadministratoren haben lediglich zur Wartung und Problembeseitigung stets Zugriff auf die verarbeiteten Daten.
- (5) Die Zugriffsberechtigungen sind in [Ziffer der Anlage] zu dieser Vereinbarung aufgelistet.

§ 13 Löschfristen

- (1) Personenbezogene Daten, für die der Verarbeitungszweck entfallen ist, werden sofort physikalisch gelöscht.
- (2) Protokolldateien werden nach fünf Tagen überschrieben und damit auch physikalisch gelöscht. Ausnahmen bedürfen der Vereinbarung.

§ 14 Besondere datenschutzrechtliche Bestimmungen

- (1) Jegliche Verarbeitung von personenbezogenen Daten wird revisionsicher protokolliert. Dies gilt auch für unberechtigte Zugriffe. Die Protokolle sind unter Verschluss zu halten.
- (2) Der betriebliche Datenschutzbeauftragte fertigt eine Datenschutzkonzeption für die Gesellschaft an, in der die technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten berücksichtigt sind. Der Betriebsrat wird diesbezüglich jeweils informiert.

(3) Der Datenschutzbeauftragte legt dem Betriebsrat und der Geschäftsleitung jährlich einen Bericht zur datenschutzrechtlichen Lage vor. In dieser ist auch auf die Aktualität der technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten einzugehen.

(4) Personenbezogene Daten, die nur für statistische Zwecke benötigt werden, sind unverzüglich zu anonymisieren.

§ 15 Beweisverwertungsverbot

Personenbezogene Daten und Erkenntnisse, die unter Verstoß gegen die Bestimmungen dieser Betriebsvereinbarung verarbeitet wurden, unterliegen einem Beweisverwertungsverbot.

§ 16 Rechte der Beschäftigten

(1) Die Beschäftigten werden über den Einsatz- und Leistungsumfang des [IT-Systems] umfassend informiert.

(2) Es wird sichergestellt, dass die Beschäftigten über den Inhalt dieser Betriebsvereinbarung informiert werden. Sie wird zusätzlich allgemein zugänglich gemacht.

(3) Alle Beschäftigte erhalten auf Wunsch einen kostenlosen Ausdruck aller über sie gespeicherten relevanten Daten in verständlicher und leicht zugänglicher Form.

(4) Die Beschäftigten werden bezüglich ihrer Rechte auf Auskunft, Berichtigung, Löschung, Widerspruch und den sonstigen Rechten der betroffenen Person aus der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes durch Schulungen und Publikationen im betriebsinternen Newsletter [mindestens jährlich] informiert.

(5) Werden von Beschäftigten gespeicherte Daten begründet beanstandet, so verpflichtet sich die Gesellschaft unverzüglich zur Korrektur. Nachteile aufgrund falscher Daten entstehen den Beschäftigten nicht bzw. sind unverzüglich rückgängig zu machen.

(6) Im Übrigen gelten die im Bundesdatenschutzgesetz und der Datenschutz-Grundverordnung geregelten „Rechte der betroffenen Person“ in der jeweils gültigen Fassung.

§ 17 Qualifizierung und Schulung

(1) Vor dem Einsatz IT-Systemen i.S.d. § 1 Abs. 3 sowie vor technischen oder organisatorischen Änderungen beim Einsatz dieser Systeme sind die betroffenen Beschäftigten rechtzeitig und umfassend über die Arbeitsmethoden und über ihre Aufgaben zu unterrichten und zu qualifizieren. Es wird ggf. ein Rhythmus zur Auffrischung der Qualifizierung zum Erhalt der Qualität festgelegt.

(2) Die Gesellschaft und der Betriebsrat entwickeln vor der Einführung von IT-Systemen i.S.d. § 1 Abs. 3 ein Qualifizierungskonzept für die Beschäftigten. Dieses beinhaltet mindestens die Lernziele, Kerninhalte, Teilnehmer/Teilnehmerinnen, Termine und Ort der Bildungsmaßnahme. Es wird ggf. ein Rhythmus zur Auffrischung der Qualifizierung zum Erhalt der Qualität festgelegt.

(3) Neue Beschäftigte werden entsprechend ihrer persönlichen Vorkenntnisse vor Arbeitsbeginn mit dem IT-System i.S.d. § 1 Abs. 3 geschult bzw. qualifiziert.

§ 18 Inkrafttreten und Kündigung

(1) Die Betriebsvereinbarung tritt am [Datum] in Kraft.

(2) Die Betriebsvereinbarung kann von beiden Betriebsparteien mit einer Frist von [drei Monaten] zum Monatsende gekündigt werden.

(3) Bis zum Abschluss einer neuen Betriebsvereinbarung gelten die vorstehenden Bestimmungen nebst Anlage fort⁶.

§ 19 Anlagen

Die Anlagen [Ziffern der Anlagen] werden Bestandteil dieser Betriebsvereinbarung. Eine Ergänzung oder Veränderung erfolgt lediglich mit dem Einverständnis beider Parteien.

§ 20 Schlussbestimmungen

(1) Ergänzungen und Änderungen dieser Betriebsvereinbarung können in beiderseitigem Einvernehmen vorgenommen werden. Sie bedürfen zu ihrer Wirksamkeit der Schriftform.

(2) Die Gesellschaft und der Betriebsrat verpflichten sich, bei Streitigkeiten, die Auslegung und Anwendung dieser Betriebsvereinbarung betreffen, unverzüglich Verhandlungen mit dem Ziel einer einvernehmlichen Regelung aufzunehmen. Im Falle der Uneinigkeit wird die Einigungsstelle angerufen. Bis zu einer Entscheidung durch die Einigungsstelle wird die beabsichtigte Maßnahme nicht durchgeführt.

(3) Sofern dies nicht ausdrücklich schriftlich erklärt wird, wird durch diese Betriebsvereinbarung keine andere Betriebsvereinbarung abgelöst. Sollten sich daraus widersprüchliche Regelungen ergeben, so sind diese in einer angemessenen Frist zu regeln.

(4) Soweit eine Bestimmung dieser Betriebsvereinbarung unwirksam sein sollte, wird die Wirksamkeit der übrigen Bestimmungen davon nicht berührt. Die unwirksame Regelung ist rechtskonform so auszulegen, dass sie dem beiderseitigen Willen der Parteien entspricht.

⁶ Die Frage der Nachwirkung der Betriebsvereinbarung bestimmt sich danach, ob es sich um eine freiwillige oder eine erzwingbare Betriebsvereinbarung i.S.d. § 77 Abs. 6 BetrVG handelt. Bei letzterer besteht eine gesetzliche Nachwirkung, wohingegen bei einer freiwilligen keine gesetzlich vorgeschriebene Wirkung besteht.