Betriebsvereinbarung über die Grundsätze zur Einführung, Nutzung und Änderung von IT-Systemen

Stand: April 2021_vBR

Inhalt

Vereinbarung

Zwischen der

XXX GmbH, yyyy Std. 3, D-89123

- nachfolgend „der **Arbeitgeber**“ oder „**AG**“ bzw. „**GF**“ -

und dem

Betriebsrat der xxx GmbH am Standort GmbH, yyyy Std. 3, D-89123

- nachfolgend „der **Betriebsrat**“ oder „**BR**“-

Wird nachfolgende Rahmen-Betriebsvereinbarung geschlossen.

1. Geltungsbereich

Diese Betriebsvereinbarung gilt für die Nutzung der bereitgestellten IT-Systeme („technische Einrichtungen"). Der genaue Geltungsbereich wird durch die Gesamtschau sowie das Zusammenspiel der folgenden Anhänge konkretisiert.

Ziel ist es, eine möglichst präzise IT- und datenschutzrechtlich konforme Definition des Unternehmens vorzunehmen:

1.1 Firma, verwandte und verbundene Unternehmen

- *Anhang 1* – Übersicht XXX Gruppe, Ultimate beneficial owner(s)
- *Anhang 2* – Organigramm XXX GmbH

1.2 Werksgelände

- *Anhang 3* - Werksplan XXX GmbH
- *Anhang 4* - Werksplan (mit technischen Einrichtungen)

1.3 Mitarbeiter

- *Anhang 5* – Mitarbeiterliste (leitende Angestellte, Tarifangestellte, Leiharbeiter, ..)
- *Anhang 6* – Userliste (Intern, Extern, Befristet, ...)
- *Anhang 12* – Rollen & Berechtigungsmodell

1.3 Hardware

- *Anhang 7* – Liste der eingesetzten Hardware

1.5 Software

- *Anhang 8* – Liste der eingesetzten Software

1.6 IT System

- *Anhang 9* – Verarbeitungsverzeichnis
- *Anhang 10* – XXX Systemtopologie
- *Anhang 13* – Domain & Hosting Konzept
- *Anhang 14* – Lösch- und Backup-Konzept
- *Anhang 15* – IT Sicherheits- & Datenschutzkonzept
- *Anhang 16* – Schnittstellen

1.7 Auftragsdatenverarbeiter

- *Anhang 9* – Liste der Auftragsdatenverarbeiter / Dienstleister
- *Anhang 10* – Drittlandabsicherungskonzept, geeignete Garantien, Übermittlungskonzept

2. Gültigkeit, Umsetzung

Das primäre Ziel der Unterlage ist es, den Schutz der Mitarbeiter vor Überwachung sowie Verhaltens- uns Leistungskontrolle im Arbeitsverhältnis zu gewährleisten und die Mitbestimmungsrechte des Betriebsrates zu wahren.

2.1 Hierarchie

Diese Rahmen-BV gilt vorrangig vor den verbundenen Einzel-BVs.

2.2 Umsetzungsverpflichtung

Die Arbeitgeberseite verpflichtet sich, etwaige technische oder organisatorische Lücken binnen der nächsten 12 Monate ab Abschluss dieser Rahmen-BV zu schließen. Es werden die Erforderlichen Verzeichnisse und Anhänge erstellt, Prozesse, Gremien und Verantwortlichkeiten definiert sowie die Freigabe unaufgefordert eingeholt und dokumentiert.

Sollte der Betriebsrat nach billigem Ermessen den Eindruck haben, dass die Umsetzung verzögert oder verwässert werden soll, steht ihm die Ausnutzung des vollen ihm zur Verfügung stehenden rechtlichen Rahmens zu.

2.3 Laufende Aktualisierung

Aufgrund der Dynamik, der das Thema unterliegt soll diese Rahmen-BV fortlaufend, jedoch mindestens 1x jährlich durch die Betriebsparteien aktualisiert werden.

2.4 Anhänge und Verzeichnisse

Anhänge sind stets, jedoch mindestens halbjährlich, durch die jeweils zuständige Fachabteilung zu aktualisieren.

2.5 Zeitpunkt

Diese Rahmen-BV tritt zum Zeitpunkt der Unterzeichnung in Kraft.

3. Grundsätze der Datenverarbeitung

3.1 Umgang mit personenbezogenen Daten

Die vorliegende Rahmen-Betriebsvereinbarung hat den Zweck, gesamthaft den Umgang mit personenbezogenen Daten in technischen Einrichtungen zu regeln.

Es werden sämtliche möglichen Gefahren für die Persönlichkeitssphäre

- organisatorisch
- technisch
- wirtschaftlich
- personell

i.S.v. §§ 87, 92-105, 106-113 BetrVG der Beschäftigten geregelt, mit dem Zweck, die Datenerhebung der personenbezogenen Daten der Mitarbeiter auf das betriebliche bzw. gesetzlich notwendige unabdingbare Maß zu beschränken.

Es muss vorrangig diejenige Option gewählt werden, die mit den geringsten Persönlichkeitsrechtseingriffen verbunden ist.

3.2 Erforderlichkeit

Bei jeder (geplanten) Verarbeitung personenbezogener Daten, die im Anhang genannten Beschäftigten / Beschäftigtengruppen betreffend, muss stets die Erforderlichkeit gem. § 26 BDSG objektiv gegeben sein. D.h. die Maßnahme muss nach billigem Ermessen beider Parteien geeignet sein, den angestrebten Erfolg (Zweck/Ziel) zu erfüllen.

Die Erforderlichkeit ist stets im engeren Sinn zu prüfen: Eine Maßnahme ist zulässig, wenn der Nachteil für den / die Beschäftigte/n und der vom AG angestrebte Erfolg nach gemeinsamen Abwägen der Parteien in einem vernünftigen Verhältnis (vgl. Fitting BetrVG § 87 Rn. 216) zu einander stehen.

Sofern gesetzlich erforderlich, wird die Speicherung, Veränderung oder Löschung von Personaldaten protokolliert.

Protokollierungen von Personaldaten, die gesetzlich nicht vorgeschrieben oder von den vom Betriebsrat freigegebenen Zwecken nicht abgedeckt sind, bedürfen der Genehmigung durch den Betriebsrat.

3.3 Zweckbezug

Eine Verarbeitung zu anderen oder anders gelagerten / weiter interpretierten Zwecken vom BR abschließend festgelegt ist untersagt. Sollten zwei oder mehr Zwecke in der Praxis kollidieren, so überwiegt stets der im Rahmen dieser BV definierte Zweck.

3.4 Beweisverwertungsverbot

Das Erheben, Verarbeiten, Kontextualisieren, Kombinieren und Nutzen sämtlicher personenbezogener Daten welche nicht von einem bestimmten und bestimmbaren ein-eindeutigen Zweck abgedeckt sind, unterliegt generell einem vorbeugendem Beweisverwertungsverbot.

3.5 Löschkonzept

Der Arbeitgeber erfasst lediglich die für vom BR definierten Zwecke zwingend notwendigen Daten und speichert diese maximal bis zu dem Zeitpunkt, an dem der Zweck erlischt. Die Löschung erfolgt stets nach DIN 66398/9 und kann vom Betriebsrat jederzeit und eigenständig kontrolliert werden.

3.6 Aufbewahrungsfristen

Die Aufbewahrungsfristen sind je nach Kategorie einzeln zu bestimmen und auf das absolut notwendige Mindestmaß zu beschränken. Gesetzlich erforderliche Fristen, etwa zu Steuer und Dokumentationszwecken, sind á Datensatz gesondert zu kennzeichnen. Eine pauschale Anwendung der gesetzliche „bis-zu-Fristen" findet nicht statt.

Audio- und Videoaufzeichnungen dürfen maximal 7 Tage gespeichert werden

Die Aufbewahrungsfrist für Backups beträgt maximal 60 Tage

3.7 Datenminimierung / Transaktionen

Die Anzahl der notwendigen Transaktionen / Datenvolumina sind stets auf das mögliche Minimum zu beschränken. Non-biometrische Single-Sign-in und Plattform-Lösungen sind zu bevorzugen.

Bei Zugriffsberechtigungen auf personenbezogenen Daten ist das Minimalprinzip einzuhalten. Jeder Mitarbeiter soll am Ende nur so viel Einblick in die Systeme und Datenbanken erhalten, wie es zur Erledigung seiner Aufgabe zwingend erforderlich ist. Personenbezogene Daten dürfen nur im Rahmen der dienstlichen Tätigkeit verarbeitet und genutzt werden. Eine Übermittlung dieser Daten oder Erkenntnissen aus diesen Daten ist nur an befugte Personen zulässig.

3.8 Ultima-Ratio

Es gilt neben dem Grundsatz der Datenminimierung / Datensparsamkeit das „Ultima ratio Prinzip", wonach sämtliche Möglichkeiten abseits einer elektronischen Datenerhebung / Überwachung (insb. bei der Erhebung audiovisueller, kommunikativer oder biometrischer Daten) zunächst vollständig und nachweislich ausgeschöpft werden müssen.

Dies ist konkret der Fall, wenn kein milderes weniger belastendes Mittel, das weniger in die Persönlichkeitsrechte des Arbeitnehmers eingreift, den gleichen oder vergleichbaren Erfolg erreichen kann, vgl. § 26 BDSG.

Die geprüften, weniger belastenden Mittel sind dem Betriebsrat vorzulegen.

3.9 Zustimmung

Jede Verarbeitung personenbezogener Daten bedarf der expliziten Zustimmung der Betroffenen.

Die erforderliche individuelle Zustimmung kann durch eine kollektivrechtliche Vereinbarung, wie z.B. Betriebsvereinbarungen, ersetzt werden. Diese ersetzt nicht den notwendigen Datenschutzhinweis an Beschäftigte.

Sämtliche Änderungen, Löschung oder Neueinführungen von technischen Einrichtungen oder Datenerhebungen bedürfen der vorherigen und expliziten Zustimmung des Betriebsrates.

Nicht mit dem BR abgestimmte Änderungen unterliegen einem vorbeugenden Beweisverwertungsverbot und können zur sofortigen Stilllegung der technischen Einrichtung führen.

Eine ausbleibende Zustimmung bzw. ein fehlender Widerspruch werden nicht als Zustimmung gewertet. Termin- und andere Vereinbarungen gelten nur dann als getroffen, wenn sie von allen Parteien Seiten jeweils bestätigt bzw. übernommen sind.

3.10 Freiwilligkeit

Die Nutzung der IT-Systeme durch die Mitarbeiter erfolgt ausschließlich freiwillig, wobei in größtmöglichem Umfang die wirtschaftliche Abhängigkeit und damit die schwächere Verhandlungsposition des Arbeitnehmers berücksichtigt wird.

Sämtliche erfolgte Zustimmungen sind schriftlich durch den Verantwortlichen zu dokumentieren. Nicht dokumentierte Zustimmungen zur Verarbeitung personenbezogener Daten gelten als nicht erteilt (nichtig).

Jeder Mitarbeiter hat die Möglichkeit, sämtliche im §34 BDSG definierten Rechte, u.a. Auskunft über ihn gespeicherte personenbezogene Daten, Empfänger der Daten und den Zweck der Speicherung individuell gegenüber dem Arbeitgeber auszuüben.

Eine Weigerung einer Einzelperson oder Personengruppe eine bestimmte technische Einrichtung zu nutzen, führt ohne die Beteiligung des BR nicht zu arbeitsrechtlichen Konsequenzen. Die Beschäftigungspflicht liegt beim Arbeitgeber.

Der Betriebsrat ist hier bereits beim Anschein der Weigerung unverzüglich hinzuzuziehen. Es ist die Aufgabe des Betriebsrates und nicht der betroffenen Person(en), mit dem AG eine einvernehmliche Lösung zu finden.

3.11 Gesundheitsschutz, Bedienergonomie

Die Parteien sind sich darüber einig, dass insb. der Gesundheitsschutz eine tragende Rolle beim Umgang mit Daten und Systemen spielt.

So besteht neben der Möglichkeit, eine Gefährdungsbeurteilung nach §87 Abs 1. Nr 7 durchführen zu lassen, der Grundsatz der Softwareergonomie:

- Bedienbarkeit,
- Praxisgerechte Abläufe,
- Vermeidung von Überwachung,
- Vermeidung von psychischem Leistungsdruck,
- Vermeidung von Arbeitsverdichtung,
- Nutzungsintensität,

werden insbesondere bei der Beschaffung und Konfiguration von IT-Systemen vorrangig berücksichtigt.

3.12 Arbeitswissenschaftliche Erkenntnisse

Als Maxime sollen stets die neusten arbeitswissenschaftlichen Erkenntnisse berücksichtigt werden. Darunter explizit

- Die Gewährung von persönlichen Freiräumen,
- planbare Tätigkeitsunterbrechungen,
- sinnvolle Arbeitsteilung,
- Erkenntnisse aus physischer und psychischer Arbeitsplatzforschung,
- Möglichst einfache User Experience / Interface,
- Beachtung menschlicher Leistungs-, Belastungs- und Kapazitätsgrenzen, sowie der
- verhältnismäßigen Handhabung und Ausübung von Kontrollrechten.

3.13 Vereinfachungen

Mögliche Systemharmonisierungen, -vereinfachungen und/oder -zusammenführungen zum Zwecke der Ergonomisierung und Effizenzierung sind Gegenstand regelmäßiger, jedoch mindestens 1x jährlicher, Überprüfungen durch die zuständigen Fachabteilungen.

Über die Ergonomisierungsvorschläge wird der Betriebsrat gesondert, anlassbezogen jedoch mindestens 1x jährlich durch die Geschäftsführung informiert.

3.14 Nichterreichbarkeit

Jeder Arbeitnehmer hat ein Recht auf Nichterreichbarkeit: Die betriebliche Kommunikation ist für einen bestimmten Zeitraum zum Schutze der Gesundheit der Mitarbeiter auszusetzen („Tot-Zeit"): Sie wird Nachts (22 - 6 Uhr) und am Wochenende (Samstag und Sonntag, Feiertag) ausgesetzt. Die Vorgesetzten sind auf diesen Verhaltensgrundsatz zu verpflichten.

Die Beteiligten vereinbaren entsprechend den Arbeitstage /-zeiten des Mitarbeiters vier Stunden Kernzeit (z.B. in der Normalschicht zwischen 10 und 14 Uhr) zu derer die Arbeitnehmer dazu angehalten werden, erreichbar zu sein.

3.15 Private Nutzung

Die technischen Einrichtungen, dürfen im Rahmen des gesetzlich erlaubten privat genutzt werden, solange der betriebsnotwendige Ablauf davon nicht gestört wird. Die Beweispflicht über das Vorliegen einer solchen Störung liegt beim Arbeitgeber.

Nicht erlaubte technische Einrichtungen und Inhalte zu sperren obliegt dem Arbeitgeber. Exzessive Nutzung oder das Verfolgen kommerzieller bzw. krimineller Absichten können zu arbeitsrechtlichen Maßnahmen führen.

3.16 Schnittstellen

Sämtliche vorhandene und potenzielle Schnittstellen (übergeordnetes oder verbundenes System, Backdoors, Webhooks, APIs, Ports, Integration Pipeline) sind explizit und im Vorfeld der Freigabe zu kennzeichnen und zu begründen.

Abweichungen von der Standardausführung sind gesondert aufzuführen und nachvollziehbar zu begründen.

3.17 Automatisierte und manuelle Entscheidungen

Jeder Mitarbeiter hat gem. §§ 54, 37 BDSG das Recht, nicht von einer automatisierten Entscheidung betroffen zu sein. D.h. ein IT-System kann immer nur eine Beratung / Stütze / Vorschlag sein, die letztendliche Entscheidung wird stets von einem biologischen Menschen getroffen und verantwortet.

Einzelentscheidungen, vornehmlich Beurteilungen, personelle Maßnahmen und Personalauswahl dürfen nicht auf der alleinigen Grundlage automatisiert erhobener Daten erfolgen.

3.18 Compliance

Die Einhaltung grundsätzlicher Compliance-Regeln wie etwa das 4-Augen-Prinzip, Principal-Agent sowie das Rotationsprinzip werden in jedem Fall und zu jedem Zeitpunkt sichergestellt und regelmäßig kontrolliert. Die mindestens zu treffenden technischen und organisatorischen Maßnahmen werden im Anhang definiert.

3.19 Integrität

Es ist seitens des Verantwortlichen sicherzustellen, dass die erhobenen Daten zu jedem Zeitpunkt die maximal mögliche Integrität (Wahrheit, Klarheit, Aktualität, Unverfälschtheit, Vollständigkeit, Nachvollziehbarkeit, Quellennachweis) aufweisen. Dem Betriebsrat sind ausschließlich integre Daten vorzulegen.

3.20 Transparenz

Dem Betriebsrat sind sämtliche Datenerhebungen sowie deren Ergebnisse transparent zu machen. Eine Datenerhebung oder Nutzung von IT-Systemen, die dem Betriebsrat ob Ihres Anlasses, Gegenstands, Umfang und Zweck nicht transparent gemacht wurde, findet nicht statt.

3.21 Privacy by Design

Sämtliche technischen Einrichtungen sind von ihrer Vor- und Grundeinstellung, spätestens ab dem Zeitpunkt der Einführung, technisch und organisatorisch primär auf den maximalen Schutz personenbezogener Daten einzurichten. Dies gilt insb. für die Anmeldung und Nutzung der Systeme durch die Mitarbeiter.

4. Mitbestimmungsrechte des Betriebsrates

4.1 Rolle des BR

Grundsätzlich hat Betriebsrat gem. § 75 Abs. 2 BetrVG die Persönlichkeitsrechte der Beschäftigten zu schützen. Er hat demnach eine Überwachungs- und Kontrollfunktion bei der Einhaltung der Arbeitnehmerschutzvorordnung gem. §80 Abs. 1 BetrVG. Es besteht ein echtes Mitbestimmungsrecht gem. § 87 Abs. 1 Nr. 6 BetrVG.

4.2 Mitbestimmungspflicht

Die Mitbestimmungspflicht besteht nach § 87 Abs. 1 Nr. 6 BetrVG bei allen technischen Einrichtungen; auf die Motive, etwa eine Überwachungsabsicht des Arbeitgebers, bzw. vorgesehenen Einsatzzweck / primäre Funktion der Einrichtung kommt es nicht an.

Für eine Mitbestimmung ist es gem. §87 Abs. 1 Nr. 6 BetrVG ausreichend, wenn eine technische Einrichtung zur Verhaltens- und Leistungskontrolle grundsätzlich geeignet ist, unabhängig von ihrem primären / originären Einsatzzweck.

Es ist für die Notwendigkeit einer Mitbestimmung hinreichend, wenn die leistungs- oder verhaltensbezogenen Daten nicht auf technischem Weg durch die Einrichtung selbst („automatisiert“) gewonnen werden, sondern manuell eingegeben und von der technischen Einrichtung weiter verwertet / gespeichert werden.

Die Mitbestimmungsrechte des Betriebsrates, gelten gem. §87 Abs. 1 Nr. 6 BetrVG auch dann uneingeschränkt, wenn lediglich ein Teil des potenziell zur Überwachung geeigneten Systems von einem Teil des Überwachungsvorgangs betroffen ist. Das Mitbestimmungsrecht des Betriebsrates bezieht sich demnach auf alle Aspekte und Teil-Aspekte der IT-Landschaft.

Neben den in §87 BetrVG geregelten Rechten gibt es weitere Beteiligungsrechte des Betriebsrates:

Um eine sinnvolle Kontrolle der Einhaltung der Regeln dieser Rahmen-BV und ihrer verbundenen Einzel-BVs sicherstellen zu können, sind sich die Parteien darüber einig dass nur ein ganzheitlicher Mitbestimmungsansatz, der sich nicht ausschließlich auf datenschutzrechtliche Aspekte bezieht, in der Praxis sinnvoll ist.

Das Mitbestimmungsrecht des Betriebsrates sieht einen präventiven Schutz vor und greift auch im Vorfeld, insbesondere bei Abwägungs- und Auslegungsfragen, beschränkt sich demnach nicht auf rein datenschutzrechtliche Aspekte.

Der Arbeitgeber hat einen Anspruch, seine Interessen hinsichtlich Gefahrenabwehr, Sicherung des Eigentums, Gestaltung der Arbeitsabläufe und Effizienzüberlegungen gemeinsam mit dem Betriebsrat erörtern.

Im Wesentlichen erstreckt sich das Mitbestimmungsrecht des Betriebsrates auf die

- Einführung
- Erhebung
- Verarbeitung
- Nutzung
- Entfernung

sämtlicher Hard- und Software sowie damit verbundener Daten.

Einschlägig und vorranging anzuwenden sind die getroffenen Definitionen im Anhang an diese BV.

4.3 Beteiligung des Betriebsrates

Der Betriebsrat ist unaufgefordert, rechtzeitig und vollständig, jedoch spätestens zu Beginn der Änderungs-, Auswahl- oder Planungsphase von technischen Einrichtungen zu beteiligen.

Grundsätzlich hat der Betriebsrat einen vollständigen Informationsanspruch um seine Mitbestimmungsrechte wirksam ausüben zu können. U.a. weil sich das Mitbestimmungsrecht auch auf teils „unwesentliche" Teilaspekte bezieht, steht es dem Betriebsrat im Einzelfall frei, welche Unterlagen und welche Intensität der Mitbestimmung er für seine jeweils erforderliche Freigabe heranzieht.

Die Einführung, Änderung oder Nutzung von technischen Einrichtungen setzt die vorherige explizite (Opt-in) Zustimmung des Betriebsrates voraus.

Der Betriebsrat erhält hierfür 6 Wochen Beratungszeit ab Einreichung der notwendigen Unterlagen gem. Freigabeprozess im Anhang.

Eine ausbleibende Zustimmung bzw. ein fehlender Widerspruch werden nicht als Zustimmung gewertet.

4.4 Kontrollmöglichkeiten des Betriebsrates

Dem Betriebsrat wird für jedes freizugebende (Teil-) System unaufgefordert eine eigene, unabhängige Kontrollmöglichkeit eingeräumt, standardmäßig durch einen eigenen, personenunabhängig nutzbaren Admin-Zugang.

Der Zugang des BR erfolgt autark und erstreckt sich auch über Systeme die vom Unternehmen genutzt werden, jedoch nicht in dessen Hoheit (Hosting, Eigentum), sondern etwa bei Dienstleistern, Auftragsdatenverarbeitern oder verbundenen / verwandten Unternehmen liegen.

Der Betriebsrat kann sich nach eigenem Dafürhalten unangekündigt, situationsunabhängig, anlasslos und selbstständig vom Zustand jedweder technischen Einrichtung überzeugen. Verträge mit Dritten sind so zu gestalten, dass die Kontrollrechte des Betriebsrates auch gegenüber Dritten wahrgenommen werden können.

Es besteht die Möglichkeit gem. §9a BDSG eine Analyse, etwa in Form eines Gutachtens durchführen zu lassen (intern oder extern), sofern der BR nach billigem Ermessen den Eindruck hat, dass möglicherweise die Integrität der personenbezogenen Daten der Mitarbeiter, eines

Teil- oder Gesamtsystems gefährdet sind. Eine vorherige Zustimmung des Arbeitgebers ist nicht erforderlich.

Selbiges gilt insbesondere auch für die Daten, Systeme und Schnittstellen des Betriebsrates selbst. Der Betriebsrat ist nicht verpflichtet, die intern vom Arbeitgeber angebotenen Mittel hierfür zu nutzen, sondern hat in jedem Fall die Möglichkeit sich selbst ein eigenes neutrales Bild zu verschaffen.

Der Betriebsrat kann nach eigenem Ermessen Gutachten für IT Systeme oder IT-Teilsysteme beauftragen. Die Begutachtung kann sowohl die eigene IT des BR, als auch die IT des Arbeitgebers zum Gegenstand haben. Die Gutachtenerstellung kann vom BR sowohl intern als auch extern beauftragt werden. Eine Zustimmung durch den Arbeitgeber ist hierfür nicht erforderlich. Die Kosten trägt der Arbeitgeber.

4.5 Sozialplan

Der Arbeitgeber verpflichtet sich, aus Anlass der Einführung und des Betriebs von IT- Systemen keine betriebsbedingten Kündigungen, Änderungskündigungen oder sonstige personelle Maßnahmen zum Zweck der Abgruppierung, sonstiger Entgeltminderung oder anderer Verschlechterung arbeitsvertraglicher Regelungen auszusprechen.

4.6 Blacklist / Whitelist

Der Betriebsrat hat die Möglichkeit

- Personen oder Personengruppen
- Produkte oder Produktgruppen
- Hersteller oder Herstellergruppen

von der (Be-)Nutzung auszuschließen („Blacklist").

Ebenfalls besteht die Möglichkeit der Beweislastumkehr mittels des Führens einer „Whitelist".

Bei Aktivierung des Whitelist-Ansatzes, sind nur noch diejenigen Personen, Hersteller oder Produkte zur Verwendung legitimiert, die Bestandteil dieser Liste sind. Die Übergangsfrist von Blacklist zu Whitelist-Ansatz soll 7 Tage betragen. Whitelist- und Blacklist-Ansatz können gleichzeitig existieren.

4.7 Bestellung DSB und Admins

Der betriebliche DSB sowie die (Teil-) Systemadministratoren werden complianceseitig als „Person of Trust" (PoTs) definiert (s. Liste anbei). Hierfür soll vor der Besetzung der Stellen ein Backgroundcheck gem. beigefügtem KYC Prozess zur Bewertung der Eignung der Personen durchgeführt werden. PoTs sind immer befristet zu berufen. Das Ergebnis der Überprüfung ist dem BR unaufgefordert vorzulegen.

Unabhängig vom Ergebnis der Überprüfung hat der BR ein echtes Mitbestimmungsrecht, konkret ein Vorschlags- und Vetorecht bei der Berufung von PoTs.

4.8 Sachverständiger

Im Hinblick auf die zunehmende Komplexität der Thematik sowie der gesetzlich erforderlichen Einbindung des Betriebsrats insb. beim Einsatz von KI und von Informations- und Kommunikationstechnik im Betrieb wird festgelegt, dass die Hinzuziehung eines Sachverständigen für Informations- und Kommunikationstechnik als erforderlich gilt.

4.9 Eigener DSB

Der BR hat die Möglichkeit für seine IT und die Sicherstellung seiner eigenen Datenschutzkonformität einen eigenen DSB zu berufen. Dieser kann sowohl intern als auch extern bestellt werden.

4.10 Autarke IT des BR

Dem BR ist eine eigene, autarke IT als Betriebsmittel zur Verfügung zu stellen. Autark heißt, frei vom Zugriff handelnder oder beauftragter Personen des Arbeitgebers. Der BR kann unabhängig und nach eigenem Dafürhalten Hard- und Software zur Eigennutzung anschaffen, installieren und nutzen. Der Arbeitgeber hat hierfür die nötigen Integrationen und Schnittstellen zur Verfügung zu stellen sowie für die Kosten der Betriebsmittel des Betriebsrates aufzukommen. Die Verwendung eigener, autarker IT setzt nicht die Zustimmung des Arbeitgebers voraus.

Der Arbeitgeber darf die Daten des BR weder selbst einsehen und auswerten noch darf er andere Personen dazu anweisen. Dem BR steht es frei, Daten durch Verschlüsselung vor unberechtigtem Zugriff zu schützen.

4.11 Gestaltungsalternativen

Der Betriebsrat kann sowohl was die personelle Besetzung, die Systemauswahl sowie zur -Nutzung Gestaltungsalternativen einbringen. Der Betriebsrat hat ein Recht auf die Erstellung sowie eine unverzügliche und schriftliche Bewertung seiner eingebrachten Gestaltungsalternativen mit Unterstützung durch den Arbeitgeber und / oder externe Experten. Eine Ablehnung der vom BR eingebrachten Gestaltungsalternative ist schriftlich zu begründen. Dem Betriebsrat steht es bei Uneinigkeit frei, die Einigungsstelle anzurufen.

4.12 Vollständige oder teilweise Stilllegung

Sollte der Betriebsrat nach billigem Ermessen Zweifel an einem neuen oder bestehenden IT-System bzw. einem Teilaspekt haben, wird dieser zweifelhafte Betriebsteil oder das Gesamtsystem mit sofortiger Wirkung, binnen 24 Stunden bis zur abschließenden Klärung stillgelegt. Die Wiederaufnahme erfolgt durch Freigabe des Betriebsrates oder einer Einigungsstellenentscheidung.

5. Rollen, Gremien Verantwortlichkeit

5.1 Verantwortlich: Der Arbeitgeber

Verantwortlich für die Durchsetzung dieser Rahmen-BV sowie ihrer verbundenen Einzel-BVs ist gem. §77 Abs. 1 BetrVG der Arbeitgeber. Die Verantwortlichkeit für Nutzung und die Vermeidung von Fehlern im Umgang mit den eingesetzten Systemen (z.B. Phishing) liegt beim Arbeitgeber.

Das Gesamtrisiko der Datenverarbeitung trägt der Arbeitgeber.

5.2 Zuständig: Der DSB

Zuständig für den korrekten Umgang mit Daten ist der betriebliche Datenschutzbeauftragte.

Die/der Beauftragte für den Datenschutz legt jährlich einen Tätigkeitsbericht vor. Das Ergebnis dieses Berichtes wird dem Betriebsrat vor der Veröffentlichung zur Verfügung gestellt.

Der DSB hat die Aufgabe, eventuellen Missbrauch in den IT Systemen systematisch zu monitoren, Verstöße zu dokumentieren und zu verhindern sowie regelmäßig, jedoch mindestens 1x im Monat bzw. anlassbezogen unverzüglich dem BR zu berichten.

5.3 Überwachung und Kontrolle: Der Betriebsrat

Der BR hat im Rahmen seiner betrieblichen Überwachungs- und Kontrollfunktion ein weitgehendes Mitbestimmungsrecht und einen Anspruch auf Durchführung der getroffenen Vereinbarung sowie auf Unterlassung vereinbarungswidriger Maßnahmen.

Es ist, soweit im Einzelfall nicht anders zwischen den Parteien vereinbart, der jeweilige örtliche Betriebsrat für alle Angelegenheiten im Sinne des §87 Abs. 1 Nr. 6 BetrVG zuständig.

Ausnahmen werden in §§ 50, 58 BetrVG (Konzernbetriebsrat) geregelt.

Es wird eine vertrauensvolle Zusammenarbeit angestrebt, der Arbeitgeber ist verpflichtet, den BR bei der Kontrolle zu unterstützen.

5.4 Kommission

Zur Umsetzung dieser Betriebsvereinbarung und zur Beilegung von Meinungsverschiedenheiten wird eine paritätisch besetzte Kommission gebildet. Sie setzt sich aus je zwei Vertretern des Arbeitgebers und zwei Vertretern des Betriebsrats zusammen. Bei Bedarf können interne oder externe sachverständige Personen beigezogen werden. Eine Zustimmung des Arbeitgebers ist hierfür nicht erforderlich.

Auf Verlagen einer der beiden Parteien tritt die Kommission unverzüglich zusammen. Die Kommission ist bestrebt, eine Klärung zeitnah herbeizuführen. Wird dieser oder einer der hier vereinbarten Grundsätze seitens einer Partei missachtet, oder hat eine Partei den Eindruck, dass dieser Anspruch unterwandert wird / werden soll, greift § 121 BetrVG uneingeschränkt.

Unberührt hiervon bleibt für beide Parteien die Möglichkeit, jederzeit die Einigungsstelle anzurufen.

5.5 Aufgaben, Verantwortlichkeiten, Rollen und Gremien

Die weiteren Rollen, Gremien und Zuständigkeiten können dem Anhang entnommen werden. Dort wird das Zusammenspiel u.a. folgender Akteure geregelt:

- IT (lokal, global)
- HR (lokal, global)
- Externe (Rechtsanwälte, Sachverständige, DSB, LDA, Auftragsdatenverarbeiter)
- IT-Ausschuss
- Compliance (internal Audit, Rechtsabteilung, …)

5.6 Konzernentscheidungen

Konzernentscheidungen bzw. die Entscheidungen verbundener oder verwandter Unternehmen finden nicht automatisch Anwendung in den von den Betriebsparteien zu beaufsichtigenden und zu führenden Unternehmen. Jede Entscheidung IT-Systeme betreffend, muss eigens, unabhängig und selbstständig für die jeweilige Unternehmung getroffen und vom BR freigegeben werden.

Zugriffe und Auswertungen auf IT Systeme des o.g. Unternehmens finden nur zu den festgelegten Zwecken und durch die vorher festgelegten Auftragsdatenverarbeiter statt. Daten oder Erkenntnisse aus Daten die durch eine nicht genehmigte Auswertung oder Zugriff erfolgten gelten als nichtig und sind unverzüglich und vollständig zu löschen. Ein Konzerndurchgriff findet nicht statt.

6.Einführung, Betrieb und Nutzung technischer Einrichtungen

Der nachfolgende Absatz soll die Bestimmungen der Einführung, Betrieb und Nutzung technischer Einrichtungen im Betrieb regeln. Im Wesentlichen wird hierzu festgehalten:

- Vor der Einführung oder Veränderung von IT-Systemen ist dem IT Ausschuss des BR die im Anhang befindliche Checkliste zur Beschlussfassung vorzustellen.
- Bei Bedarf ist auf Beschluss des Betriebsrats ein Sachverständiger hinzuzuziehen.
- Die Einführung, Nutzung oder Änderung einer technischen Einrichtung bedingt der vorherigen expliziten (Opt-in) Zustimmung des Betriebsrates.
- Der Betriebsrat hat Anspruch auf Herausgabe sowie persönlicher Erläuterung aller notwendigen Informationen. Die Informationen müssen stets vollständig und in aktuellster Fassung („integer") vorgelegt werden.
- Die gesetzlich vorgeschriebene Vorabkontrolle ist durch die/den Beauftragte/n für den Datenschutz durchzuführen.

6.1 Informationsanspruch

Die im Anhang befindliche Liste ist ein Auszug dessen, welche Informationen der Betriebsrat u.a. für die Freigabe der Einführung, Nutzung oder den Betrieb von IT-Systemen verlangen kann.

Da die Thematik der Digitalisierung generell einer enormen Dynamik untersteht, soll diese Liste einen Eindruck vom Detaillierungsgrad sowie den Umfang der möglichen Fragen zum Zeitpunkt der Erstellung dieser BV vermitteln.

Welche Informationen der BR für seine Entscheidungsfindung genau heranzieht bleibt im Einzelfall dem Betriebsrat selbst überlassen. Die in den Absätzen 4.3. und 4.4. (Beteiligungs- und Kontrollrechte des BR) genannten Rechte bleiben hiervon unberührt.

Eine Zensur findet nicht statt.

6.2 Roll-out

Der genaue Prozess der Einführung, Änderung und Nutzung von IT Systemen („Roll-Out") ist im Anhang definiert.

Dem Betriebsrat ist auf Nachfrage eine eigene Testumgebung („Sandbox") einzurichten bzw. Hardware-Protoypen zum Verbleib im Besitz des Betriebsrates auszuhändigen.

Jede Abweichung von Standardsoftware sowie Schnittstellen ist explizit zu Kennzeichnen und dem Betriebsrat unaufgefordert und im Vorfeld der Nutzung zur Anzeige zu bringen. Die in Abs. 3.16. getroffenen Regelungen bleiben hiervon unberührt.

Eine Änderung / Einführung / Löschung eines Systems oder Teilsystems ohne schriftliche und explizite Freigabe des Betriebsrates während oder nach der Einführung findet nicht statt.

Die Zustimmung der Arbeitnehmervertretungen zu Voruntersuchungen oder Probeläufen besitzt keine präjudizierende Wirkung für die spätere Einführung eines Systems oder Teilen davon.

Die Freigabe von (Teil-) Systemumfängen durch einzelne Betriebsräte ist nicht vorgesehen. Alleine die in Beschlussfassung vorliegende Zustimmung des BR ist für eine Freigabe maßgeblich.

6.3 Kommunikation

Eine Änderung / Nutzung / Löschung / Einführung von IT-Systemen ohne vorherige Kommunikation findet nicht statt. Es müssen vor jeder Systemänderung mindestens die betroffenen Personen sowie deren Vorgesetzte informiert werden.

Der Betriebsrat hat jederzeit das Recht, ein geeignetes Kommunikationskonzept, auch ex-post, einzufordern. Die Kommunikation muss über geeignete Medien, wahrheitsgemäß, in geeigneter Sprache und zugänglich für alle Betroffenen erfolgen. Auf Datenschutzrechtliche Implikationen muss hingewiesen werden.

Beide Parteien sind sich darüber einig, dass von einer Kommunikation, die Projektverzögerungen oder etwaige Mehrkosten „zu Lasten des Betriebsrates“ legt (z.B. „keine Freigabe des Betriebsrates“) seitens aller Beteiligten bis zur vollständigen und abschließenden Entscheidung durch den Betriebsrat, im Hinblick auf die Sicherung des Betriebsfriedens, Abstand genommen wird. Die Geschäftsführung wird die Fachverantwortlichen vor Beginn jedes Projektes auf diesen Grundsatz verpflichten.

Bei Zuwiderhandlungen greift § 121 BetrVG. Der BR ist hierbei befugt, arbeitsrechtliche Maßnahmen zu ergreifen.

Der Betriebsrat darf zum Zwecke der Kommunikation mit der Belegschaft sämtliche technischen Einrichtungen nach billigem Ermessen selbstständig nutzen.

6.4 Datenschutzhinweis an Beschäftigte

Die notwendige Information über die Verarbeitung der persönlichen Daten der Betroffenen wird den Betroffenen im Vorfeld der Einführung zugänglich gemacht. Sie ist dem Betriebsrat vor der Verteilung unaufgefordert zur Freigabe vorzulegen. Die jeweils aktuelle Version des „Datenschutzhinweis an Beschäftigte“ ist jederzeit für jeden Betroffenen abrufbar.

Der „Datenschutzhinweis an Beschäftigte“, enthält die genauen im jeweiligen IT-System verarbeiteten personenbezogenen Daten, deren Zweck, die Löschfristen sowie die gesetzlich vorgesehenen Möglichkeiten nach §34 BDSG. Er muss in schriftlicher Form von den Betroffenen entgegengenommen werden. Die Entgegennahme des Datenschutzhinweises ist schriftlich durch die Betroffenen zu bestätigen.

Die Zustimmungs-Verwaltung („Consent Management“) liegt in der Verantwortung des betrieblichen DSB und kann jederzeit vom BR kontrolliert werden.
Änderungen werden den Betroffenen unaufgefordert und vor deren Wirksamwerden mitgeteilt.

6.5 Qualifizierung

Den Betriebsparteien ist es ein gemeinsames Anliegen, die Mitarbeiter auf dem Weg der Digitalisierung zu qualifizieren und die digitale Kompetenz nachhaltig und wo nötig individuell zu fördern.

Es wird daher vereinbart, jährlich mindestens xx% der Investitionen in Hard- und Software in die IT-Kommunikation sowie die IT-Qualifizierung der Mitarbeiter zu investieren.

Vor der Einführung von IT-Systemen ist mit dem Betriebsrat ein Qualifizierungskonzept abzustimmen. Hierin sind mindestens die

- Lernziele,
- Kerninhalte sowie der
- Teilnehmerkreis

enthalten. Das Qualifizierungskonzept enthält, abhängig vom Einsatzzweck des jeweiligen IT-Systems, auch Beschreibungen über die

- ergonomische Gestaltung („User Experience") und
- Grundsätze des Datenschutzes sowie der
- Datensicherheit.

Der Betriebsrat hat jederzeit das Recht, ein Schulungs- bzw. Qualifizierungskonzept, auch ex-post, einzufordern.

Der gesetzliche Schulungsanspruch des Betriebsrates nach § 37 Abs. 6 bleibt hiervon unberührt.

Die Anwender einer technischen Einrichtung werden aufgabengerecht und ausschließlich während der Arbeitszeit qualifiziert. Die Kosten trägt der Arbeitgeber.

Jeder User hat Anspruch auf eine Schulung im Vorfeld der Nutzung. Kein Mitarbeiter wird verpflichtet ein IT-System zu nutzen, für das er im Vorfeld keine ausreichende Qualifizierung erhalten hat. Die Beweislast hierüber liegt beim Arbeitgeber.

Grundsätzlich soll jede Qualifizierungsmaßnahme in zeitlich enger Koppelung mit der Einführung oder Änderung der technischen Einrichtung stattfinden. Auswertungen, wie etwa „Pre- und Post-Tests" sowie Umfragen sind vor ihrer Durchführung separat durch den Betriebsrat genehmigungspflichtig.

Die Qualifizierungsmaßnahme erfolgt in deutscher Sprache, wenn nicht die Durchführung in einer anderen Sprache sinnvoll ist.

7. Überwachung, IT Compliance

7.1 Überwachung

Eine systematische, automatische oder stichprobenartige Überwachung, Filterung, Kontextualisierung, Verbindung oder Sortierung („Raster-Fahndung“) der Inhalte und Nutzungsdaten findet nicht statt. Dies gilt insbesondere für Kommunikations-, IT-, Personal-, Finanz- und audiovisuelle Systeme.

Die Parteien sind sich darüber einig, dass jedweder Anschein von verdeckter oder offener Überwachung („Überwachungsatmosphäre“) bei der Nutzung der technischen Einrichtungen präventiv und bereits im Vorfeld vermieden werden soll.

Die festgelegten Zwecke für die notwendige Überwachung zur Sicherung der legitimen Interessen des Arbeitgebers wird im Anhang definiert. Sämtliche darüber hinaus gehenden Erfassungen, Aufzeichnungen, Nutzung oder Auswertungen oder Erkenntnisse daraus sind nicht gestattet.

7.2 Verhaltens- und Leistungskontrolle

Eine Verarbeitung zum direkten oder indirekten (mittelbaren oder unmittelbaren) Zweck der Verhaltens- und Leistungskontrolle findet nicht statt.

Der Arbeitgeber kann personenbeziehbare, personenbezogene und besonders personenbezogene (nachfolgend: „personenbezogene“) Daten für die Anbahnung, Begründung und Durchführung des Beschäftigungsverhältnisses wie im Anhang spezifiziert erheben, verarbeiten und nutzen. Die Nutzung muss stets im engstmöglichen zeitlichen und inhaltlichen Zusammenhang mit der vom Gesetzgeber verlangten und mit dem Betriebsrat abgestimmten Zweckbestimmung gem. Anhang stehen.

7.3 Bonus / Malus-System

Für den Betrieb von Bonus- / Malus Systemen sei auf die jeweils geltenden Einzel-BVs verwiesen.

Die Rechte des Betriebsrates nach § 87 Abs. 1. Nr 6, 8 und 11 sowie §§ 92, 94, 95 BetrVG bleiben hiervon unberührt.

7.4 Elektronische Personalakte

Die Regelungen zur Elektronischen Personalakte können der Betriebsvereinbarung „E-Personalakte“ entnommen werden.

Die eingangs aufgeführten Kontrollrechte des BR gelten uneingeschränkt.

7.5 Auswertungen

Auswertungen, die außerhalb oder zusätzlich zu den im Anhang definierten Zwecken erfolgen sollen, bedingen der vorherigen expliziten („Opt-in“) schriftlichen Zustimmung des Betriebsrates.

Auswertungen und Zugriffe, die nicht vom erforderlichen Zweckbezug im Anhang abgedeckt sind, oder vom BR freigegeben wurden sind vollständig untersagt.

Unbefugt erfolgte Zugriffe oder Auswertungen sind dem Betriebsrat unverzüglich anzuzeigen und können zu arbeitsrechtlichen Konsequenzen gegen Einzelpersonen und/oder Verantwortliche bzw. Vorgesetzte führen.

7.6 Prognosedaten

Die Erstellung und Verwendung von Prognosedaten („Predictive Data") findet nur zu den genehmigten Zwecken bzw. im Rahmen der genehmigten Auswertungen statt. Die Erstellung, Erhebung, Kontextualisierung, Fortschreibung und Nutzung von Daten oder Erkenntnissen aus Daten zur / der Prognose bedarf der gesonderten Zustimmung des BR.

7.7 Profiling

Das automatisierte oder analoge Anlegen von Profilen jedweder Couleur, vorrangig Verhaltens-, Nutzungs-, biometrische-, Bewegungs-, Leistungs- und Persönlichkeitsprofile findet nicht statt. Dies gilt insbesondere für Finanz-, Gesundheits-, CRM-, ERP-Systeme sowie die (E-) Personalakte(n).

7.8 BYOD

Die Parteien sind sich einig darüber, dass für die User die Möglichkeit geschaffen werden soll, an den betrieblichen Abläufen über eigene (private) Devices teilzunehmen („BYOD"). Einzelheiten hierzu können der BV „BYOD" entnommen werden.

7.9 Mobile Device Management

Sämtliche im Einsatz befindliche Hard- und Software wird ihm Rahmen eines Mobile Device Management Systems erfasst und verwaltet. Details hierüber lassen sich der BV „Mobile Device Management" entnehmen.

7.10 Mobiles Arbeiten

Die Parteien sind sich darüber einig, dass sämtliche Arbeitsplätze, wo immer möglich (mit angemessenem Aufwand unter Beachtung von technischen und Risikoaspekten), mobil arbeitsfähig zu gestalten sind.

Die Details zur Regelung können der BV „Mobile Arbeit" entnommen werden.

7.11 Ermittlungen

Zur Aufdeckung von Straftaten oder der Durchführung interner Ermittlungen dürfen personenbezogene Daten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Einzelperson im Beschäftigungsverhältnis eine Straftat begangen hat, die Datenverarbeitung zur Aufdeckung erforderlich ist („Ultima-Ratio") und das schutzwürdige Interesse des Mitarbeiters nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig oder gegenüber Dritten diskreditierend sind. Im Übrigen sind die Regelungen des § 26 BDSG einschlägig.

- Der Betriebsrat ist in jedem Fall zum frühestmöglichen Zeitpunkt hinzuzuziehen
- Das datenbasierte Ermitteln im Unternehmen setzt in jedem Fall notwendigerweise die Eröffnung eines Verfahrens voraus.

- Einzelpersonen erfahren bis zur vollständigen Klärung des Sachverhaltes keine arbeitsrechtlichen Konsequenzen.

7.12 Auswertungen und Beteiligung des Betriebsrats

Bei der individuellen Prüfung von Personaldaten ist eine gesonderte vorherige Zustimmung des Betriebsrates einzuholen. Der Betriebsrat erhält seitens der mit der Prüfung beauftragten Stelle alle erforderlichen Informationen über die beabsichtigte Prüfung und nimmt daran teil (4-Augen-Prinzip).

Bei Gefahr im Verzug kann ohne seine Anwesenheit, jedoch nur mit vorheriger Zustimmung des Betriebsrates überprüft werden. Der Betriebsrat ist in jedem Fall unverzüglich hinzuzuziehen.

Personelle Maßnahmen, die auf Informationen (auch zufälligen, „Beifang") beruhen, die unter Verletzung dieser Betriebsvereinbarung gewonnen wurden, sind, abgesehen von den Vorschriften des StGB, unwirksam, sie unterliegen konkret einem Beweisverwertungsverbot und müssen unverzüglich vernichtet werden.

7.13 Zugriffe

Zugriffsberechtigungen werden ausschließlich gemäß des genehmigten Rollen- und Berechtigungskonzeptes erteilt. Die Zugriffe haben sich stets auf das erforderliche Minimum zu beschränken. Zugriffe finden ausschließlich zu den im Anhang festgelegten Zwecken statt.

Nicht mehr benötigte Berechtigungen sind sofort mit Erlöschen des Zweckes zu Entziehen. Überberechtigungen sind unverzüglich bei Bekanntwerden zu entziehen.

Das Agieren von Personen in technischen Einrichtungen der Organisation, die nicht in dem genehmigten Rollen- und Berechtigungskonzept gelistet sind, bedarf der vorherigen Freigabe des Betriebsrates.

Das Verarbeiten via „Bypassen" (Zugriff / Änderung / Anbindung) von Systemen etwa durch ein übergeordnetes oder verbundenes System, Backdoors, Webhooks, APIs, Ports, verebte Rechte … abseits des definierten Freigabeprozesses sowie eine Zweckentfremdung, variierend oder über die im Anhang definierten Zwecke hinaus, ist nicht zulässig.

Unbefugt erfolgte Zugriffe, Verstöße oder das Vorliegen von Informationen über Verstöße oder Änderungen an den freigegebenen Systemen sind dem Betriebsrat unverzüglich anzuzeigen und können zu arbeitsrechtlichen Konsequenzen gegen Einzelpersonen und/oder Verantwortliche bzw. Vorgesetzte führen.

Die Mitarbeiter, insbesondere die Mitarbeiter der Personal-, Finanz- und IT-Abteilungen, werden im Rahmen regelmäßiger Schulungen im Vorfeld der Nutzung auf dieses Zweckentfremdungs- und laterale Nutzungsverbot durch den Arbeitgeber sensibilisiert.

Zugriffsberechtigungen werden ausschließlich befristet erteilt. Das Rotationsprinzip sowie das Vier-Augen-Prinzip finden zu jedem Zeitpunkt vollständig Anwendung.

7.14 Verpflichtung auf das Datengeheimnis

Sämtliche mit den IT-Systemen betraute Personen sind nachweislich und schriftlich auf das Datengeheimnis zu verpflichten. Dies gilt insbesondere für die Mitarbeiter in den Bereichen IT, Personal, PoT und Finanz. Die Verantwortung zur Verpflichtung sowie der Führung der schriftlichen Nachweise darüber liegt beim Arbeitgeber.

Jede mit der Datenverarbeitung betraute Person ist gegenüber dem Betriebsrat wahrheitsgemäß und vollständig mitwirkungs- und auskunftspflichtig. Die Auskunft führt für die Beschäftigten zu keiner arbeitsrechtlichen Benachteiligung.

7.15 Bewerbungsprozess

Im Rahmen des Bewerbungsprozess soll ein strenges Neutralitätsgebot eingehalten werden. Es ist untersagt, interne oder externe Bewerber zu googeln, bzw. deren Social Media Aktivitäten zu recherchieren.

Etwaige Daten oder Erkenntnisse aus Daten, die nicht explizit und freiwillig vom Bewerber selbst zum Zwecke der Bewerbung übermittelt wurden, fließen ohne die Zustimmung des Betroffenen nicht in die Entscheidungsfindung ein.

Sollte im Einzelfall, etwa bei der Besetzung von Stellen die als PoT gekennzeichnet sind, eine erweiterte Hintergrundüberprüfung nötig sein, so gelten die Bestimmungen aus dem Anhang „Recruiting Policy".

In jedem Fall ist vor der Prüfung erweiterter Informationen über Bewerber der Betriebsrat zum frühestmöglichen Zeitpunkt vollständig hinzuzuziehen.

7.16 Anonymisierung und Pseudonymisierung

Wenn die Verarbeitung personenbezogener Daten zwingend erforderlich ist, werden sämtliche Daten, wo immer möglich, anonymisiert und pseudonymisiert.

Den Regelungen des Anonymiserungs- und Pseudonymisierungskonzeptes im Anhang wird zu jedem Zeitpunkt vollumfänglich und auch bei Dritten einfach überprüfbar Rechnung getragen.

Insbesondere bei personenbeziehbaren Daten ist auf die Qualität der Anonymisierung besonders Wert zu legen: Eine „Rückwärts-Personifizierung" („Reverse Engineering") die einen Bezug bzw. Rückschluss auf das Verhalten von Einzelpersonen bzw. Personengruppen zulässt, erfolgt ohne vorherige Genehmigung durch den Betriebsrat nicht.

7.17 Leaks, Hinweisgebersysteme

Systemabstürze, Leaks, Downtimes und andere systembedingte Arbeitsunterbrechungen sind dem Betriebsrat unverzüglich und unaufgefordert zu melden. Jeder Arbeitnehmer hat hierbei die Pflicht, ihm zur Kenntnis erlangte Verstöße gegen den Geist dieser und der verbundenen BVs unverzüglich zu melden.

Hierfür stehen die im Anhang genannten neutralen Stellen zur Verfügung, an der anonym Hinweise eingehen können. Der Schutz von Whistleblowern hat hierbei stets oberste Priorität, arbeitsrechtliche Konsequenzen können durch die korrekte Nutzung der Hinweisgebersysteme nicht entstehen.

Die Ansprechpartner werden jedem Mitarbeiter regelmäßig mitgeteilt sowie die Vorgesetzen in der Jahreszielvereinbarung auf die Kommunikation der Hinweisgebersysteme und deren Nutzung verpflichtet.

Einzelne Mitarbeiter, mit Ausnahme von Geschäftsführern oder leitenden Angestellten, können, sofern kein grob fahrlässiges oder vorsätzliches Handeln nachgewiesen wurde, für Systemabstürze, Downtimes und andere systembedingte Arbeitsunterbrechungen am oder im IT System nicht persönlich haftbar gemacht werden. Alle diesbezüglichen Unterbrechungen gehen nicht zu Lasten der Arbeitszeitkonten der Beschäftigten.

7.18 Videoüberwachung

Der Arbeitgeber hat das Recht, sein Eigentum etwa mittels Videoüberwachung zu schützen. Einzelheiten über die Erhebung, Erfassung und Nutzung von Videodaten sowie deren Speicherung, Zugriff und Löschung können der BV „Video" entnommen werden.

Eine Aufzeichnung von Videokonferenzen jedweder Art findet nicht statt. Sollte dies im Ausnahmefall erforderlich sein, hat der Betriebsrat die zeitlich und im Umfang begrenzte, zweckbezogene und nach Prüfung sämtlicher milderer Mittel, Maßnahme durch den Arbeitgeber, im Vorfeld der Aufzeichnung freizugeben.

7.19 E-Mail

Eine Überwachung von Email-Postfächern, allen voran der Inhalte findet nicht, auch nicht auf Meta- oder Indexierungsebene statt. Weitere Details können der BV „Microsoft 365" entnommen werden.

7.20 Cloud

Die Nutzung von europäischen (Hosting in Europa) Cloud Anbietern ist grundsätzlich gestattet. Die genauen Regelungsabreden hierzu, insbesondere was Drittlandabsicherungskonzepte und geeignete Garantien für die Datenübermittlung angeht, können der BV „Cloud Computing" entnommen werden.

7.21 Browser

Die Nutzung von Browsern soll auf diejenigen Produkte beschränkt werden, deren Erhebung personenbezogener Daten sich auf das Minimum beschränkt. Individualisierbare Browser sind zu vermeiden. Sollten bestimmte Umstände (etwa technische Voraussetzungen) einen anderen, als den datensparsamsten Browser erfordern, so ist dieser, dessen Individualisierung und Schnittstellen, separat vom Betriebsrat im Vorfeld der Nutzung freizugeben. Weitere Regelungen lassen sich der BV „Internetnutzung" entnehmen.

7.22 Listen, Namensschilder und Dienstpläne

Listen, etwa

- Geburtstagslisten
- Jubiläumslisten
- Namenslisten

sind auf das notwendige Minimum zu Beschränken und so zu verwahren, dass lediglich diejenigen Personen, die mit dem jeweiligen Vorgang aktiv betraut oder betroffen sind, nur für den notwendigen Zeitraum Einblick erhalten.

So sollen, sowohl bei Listen, als auch bei Namensschildern lediglich der

- Nachname sowie der
- erste,
- bei gleichnamigen Mitarbeitern jeweils ein weiterer Buchstabe des Vornamens erfasst werden.

Bei Geburtstagslisten ist es, mit Zustimmung durch die Betroffenen, hinreichend, lediglich das Datum, ohne das Geburtsjahr zu erfassen.

Dienstpläne sind so zu gestalten, verteilen und zu bearbeiten, dass jeder Mitarbeiter jeweils nur seinen eigenen, ihn betreffenden individuellen Dienstplan einsehen kann. Abweichende Regelungen, etwa innerhalb von Fertigungsgruppen, können auf Antrag getroffen werden, bedürfen der vorherigen Freigabe durch den Betriebsrat.

Jeder Mitarbeiter hat auf Wunsch das Recht auf Pseudonymisierung, Anonymisierung sowie Anspruch auf weitere, im § 34 BDSG geregelte Rechte.

8. Zuwiderhandlung, Eskalation

8.1 Zuwiderhandlung

Eine Zuwiderhandlung liegt vor, wenn eine der beiden Parteien nach billigem Ermessen der Ansicht ist, dass gegen eine oder mehrere Regelungen dieser Rahmen-BV oder einer ihrer verbundenen BV's bzw. deren Regelungsgeist verstoßen wurde.

Eine Zuwiderhandlung kann durch beide Seiten auch bei drohender Gefahr präventiv unterbunden werden. Die jeweilige Definition von drohender Gefahr obliegt dem billigen Ermessen der jeweiligen Partei.

Etwaige Vorwürfe über Verstöße im Zusammenhang mit der der Nutzung von IT-Systemen gelten als widerlegt, wenn zwei übereinstimmende Willenserklärungen vorliegen. Eine Partei kann nicht einseitig Vorwürfe oder Ermittlungen als nichtig, unwesentlich, abgeschlossen oder erledigt erklären.

8.2 Eskalationsprozess

Im Falle einer Zuwiderhandlung greift der in Anhang definierte Eskalationsprozess. Siehe hierzu auch 6.3 „Kommission"

Schlussbestimmungen

Ablösung

Diese Betriebsvereinbarung löst die Rahmenbetriebsvereinbarung über den Einsatz von IT Systemen vom 3.3.2010 mit der Maßgabe ab, dass die insoweit genehmigten IT-Systemen weiter betrieben werden dürfen.

Für alle bislang bestehenden bzw. eingesetzten IT- Systeme verpflichten sich Geschäftsleitung und Betriebsrat bis zum 31.12.2021 entsprechende IT- Steckbriefe zu erstellen.

Verbundene Betriebsvereinbarungen

Sollte für die Einführung, Nutzung oder Änderung von IT-Systemen einzelfallbezogene Regelungen erfordern, erfolgt ein gesonderter Abschluss einer Betriebsvereinbarung bzw. die Erweiterung dieser Rahmen BV.

Alle in dieser Betriebsvereinbarung aufgeführten Anlagen sind Bestandteil der Vereinbarung.

Ex-Post

Sämtliche in dieser Rahmen-BV getroffenen Regelungen gelten sowohl für bereits existierende Systeme (ex-post) als auch zukünftige Aktivitäten (ex-ante).

Salvatorische Klausel, Inkrafttreten und Geltungsdauer

Sollte eine Bestimmung dieser Betriebsvereinbarung unwirksam oder undurchführbar sein, berührt dies nicht die Wirksamkeit der übrigen Bestimmungen. Arbeitgeber und Betriebsrat werden kurzfristig Verhandlungen aufnehmen mit dem Ziel, eine einvernehmliche Lösung dieser Punkte zu erarbeiten.

Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft und kann mit einer Frist von 3 Monaten zum Monatsende gekündigt werden. Ihre Regelungen gelten weiter, bis sie durch eine neue Abmachung ersetzt werden.

Unterschriften

_____

Christoph Stoller

Geschäftsführer

_____

Ina Schneemann

Betriebsratsvorsitzende

_____

Halka Steiper

Cluster HR Director

_____

Christof Pfarr

Stellvertretender BR-Vorsitzender

, den xx. April 2021

Anhänge / Verzeichnisse

1 Mindestanforderungen an technische & organisatorische Compliance
2 Freigabeprozess Einführung technische Einrichtungen
3 Unterlagen für die Freigabe
4 KYC Prozess
5 PoT Liste
6 Rollen & Berechtigungsmodell
7 Zugriffsliste
8 Verarbeitungsverzeichnis
9 Blacklist / Whiteliste
10 Liste der Auswertungen
11 Löschkonzept
12 Gremien & Aufgaben
13 Eskalationsprozess
14 Hinweisgebersystem
15 Genehmigte Überwachungsumfänge
16 Definitionen
17 Anonymisierungs- / Pseudonymisierungskonzept
18 Datenkategorien
19 Empfänger / Kategorien von Empfängern

Verbundene BVs

1 BV BYOD

2 BV Mobile Device Management

3 BV Internetnutzung

4 BV Microsoft 365

5