Arbeit und Technik

RAHMENVEREINBARUNG DATENSCHUTZ

Rahmen-Betriebsvereinbarung
Stand 2023

www.gpa.at

gpa MEINE GEWERKSCHAFT

Vorbemerkung: Mustervereinbarungen und Leitfäden können Orientierung geben, sind jedoch nur dann nützlich, wenn sie auf die speziellen betrieblichen Umstände zugeschnitten sind. Wird ein Betriebsvereinbarungsmuster nicht „maßgeschneidert", gehen schnell wichtige Gestaltungsmöglichkeiten verloren. Aus diesem Grund sind die Regelungen der nachfolgenden Betriebsvereinbarung als Eckpunkte zu verstehen. Sie sollen als Anregungen dienen, um daraus eine zu den Verhältnissen im eigenen Betrieb optimal passende Vereinbarung zu entwickeln. Die GPA unterstützt und berät gerne auf diesem Weg!

Hinweis: Die in der Muster-Betriebsvereinbarung grau hinterlegten Passagen sind als erläuternde Kommentare zu verstehen oder weisen auf alternative Vorgangsweisen hin.

RAHMENBETRIEBSVEREINBARUNG

über die Verwendung personenbezogener Daten von Beschäftigten

abgeschlossen zwischen dem Unternehmen XY einerseits und

dem zuständigen Betriebsrat

Das kann sein: der Arbeiter- und/oder Angestelltenbetriebsrat, der Betriebsausschuss oder auch der Zentralbetriebsrat [nach Kompetenzübertragung]

Inhalt

Präambel

IT-Systeme[1], die personenbezogene Beschäftigtendaten verwenden, benötigen eine datenschutzrechtlich- und arbeitsrechtlich konforme Grundlage. Laut § 96 und § 96a Arbeitsverfassungsgesetz (ArbVG) sind bei der Verwendung von personenbezogenen Daten in Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten sowie bei Kontroll- und Überwachungssystemen Betriebsvereinbarungen abzuschließen.

Aufgrund der technologischen Schnelllebigkeit und häufiger Veränderungen in der Funktionalität der eingesetzten IT, soll ein abgestuftes Regelungskonzept angewendet werden, das diesem technischen Fortschritt entgegenkommt, ohne rechtliche Anforderungen zu untergraben.

In der Rahmenbetriebsvereinbarung (RBV) zur Verwendung personenbezogener Daten im Betrieb werden daher allgemeine, systemunabhängige Regelungen vereinbart. Darunter fallen z.B. der Umgang mit BenutzerInnendaten, die in allen IT-Systemen anfallen, unternehmensweite Regelungen zur Einhaltung des Beschäftigtendatenschutzes, die Mitgestaltungs- und Kontrollrechte des Betriebsrates.

Die Rahmenbetriebsvereinbarung wird ergänzt von Zusatzbetriebsvereinbarungen zu den konkreten, im Einsatz befindlichen bzw. geplanten IT-Systemen (z.B. Zeiterfassung, Zutrittskontrolle, Kommunikations- und Kollaborationssysteme, Videokontrolle;). Die Rechtswirkung entsteht durch die Kombination von Rahmenbetriebsvereinbarung und System-Betriebsvereinbarung.

1. Geltungsbereich

Diese Betriebsvereinbarung gilt:

[1] Unter dem Begriff Informationstechnisches System (IT-System) versteht man jegliche Art elektronischer datenverarbeitender Systeme. Darunter fallen zum Beispiel Computer, Großrechner, Serversysteme, Datenbanksysteme, Informationssysteme, Prozessrechner, Digitale Messsysteme, eingebettete Systeme, Mobiltelefone, Handhelds, Videokonferenzsysteme und diverse Kommunikationssysteme u.a.m.

Personell: für alle ArbeitnehmerInnen, VolontärInnen und freien DienstnehmerInnen sowie natürliche Personen im Sinne des § 36 ArbVG [d.h. Zeitarbeitskräfte, überlassene ArbeitnehmerInnen sowie HeimarbeiterInnen sind eingeschlossen].

Sachlich: allgemeine technische, organisatorische und personelle Regelungen für die Planung, Einführung und Verwendung bestehender und zukünftiger informationstechnischer Systeme (IT-Systeme), die personenbezogenen Daten von Beschäftigten verarbeiten.

Die Grundsätze dieser Rahmenbetriebsvereinbarung gelten für alle (auch zukünftige) Zusatzbetriebsvereinbarungen, die den konkreten Einsatz von IT-Systemen beschreiben (Betriebsvereinbarungen im Sinne der §§ 96, 96a und 97 ArbVG).

Regelungen zu den jeweiligen IT-Systemen werden in den folgenden Anhängen beschrieben:

- Anhang 1: Übersicht der IT-Systeme, die personenbezogene Daten von Beschäftigten verarbeiten und für die die Regelungen der Rahmenbetriebsvereinbarung ausreichend sind. Mindestinhalte pro System sind in einem Datenblatt zu erfassen.
- Anhang 2: Übersicht der IT-Systeme, die bereits durch eine (Zusatz-)Betriebsvereinbarung geregelt sind.
- Anhang 3: IT-Systeme, die durch eine (Zusatz-)Betriebsvereinbarung geregelt werden. Basis für die Regelung dieser Systeme sind die Informationen wie in Anhang 3 beschrieben

2. Rechtsgrundlagen und Begriffsdefinitionen

Die rechtliche Basis bilden:

- die Bestimmungen des Arbeitsverfassungsgesetzes (ArbVG), im Besonderen die §§ 89, 91, 92, 96, 96a und 97
- die Bestimmungen der EU-Datenschutzgrundverordnung und des
- Datenschutzgesetzes (DSG)
- die Bestimmungen des ArbeitnehmerInnenschutzgesetzes (ASchG)
- [Im Zusammenhang mit IKT-Einsatz insbesondere §68 zur benutzergerechten Gestaltung von Bildschirmarbeitsplätzen wichtig, wobei auch die Bildschirme von diversen mobilen Geräten gemeint sind.]
- das Kommunikationsgeheimnis nach § 161 Abs 3 Telekommunikationsgesetz (TKG 2021)

Die Definitionen aus der Europäischen Datenschutzgrundverordnung (DSGVO) und des Datenschutzgesetzes (DSG) finden in dieser Betriebsvereinbarung Anwendung.

3. Zielsetzung

Diese Betriebsvereinbarung dient zur Qualitätssicherung und Transparenz bei der Verwendung personenbezogener Daten beim Einsatz von IT-Systemen. Sie kann Betriebsvereinbarungen zu einzelnen IT-Systemen nicht ersetzen, gibt aber einen Rahmen vor. Personenbezogene Daten von Beschäftigten dürfen nur verwendet werden, soweit der Verwendungszweck rechtlich gedeckt ist.

Es besteht Übereinstimmung darüber, dass der Einsatz von IT-Systemen dazu dient, die sich aus Gesetzen, Kollektivverträgen, Betriebsvereinbarungen oder Arbeitsverträgen ergebenden Aufgaben des Arbeitgebers zu unterstützen und zu erleichtern.

Es besteht weiters Konsens, dass bei der Verarbeitung von personenbezogenen Daten von Beschäftigten ein entsprechender Schutz geboten wird vor

- einer systematischen, die Menschenwürde des Einzelnen berührenden Kontrolle,
- unberechtigten Leistungs- und Verhaltenskontrollen,
- unerlaubter Erstellung eines personenbezogenen Profiling,
- unberechtigter Speicherung, Übermittlung und Offenlegung von personenbezogenen Daten.

4. Grundsätze der Datenverarbeitung im Beschäftigungskontext

Der Arbeitgeber stellt die Einhaltung der Datenschutzgrundsätze nach folgenden Prüfmaßstäben sicher und informiert den Betriebsrat darüber:

- **Transparenz**: Über jedes IT-System, das personenbezogene Daten von Beschäftigten verarbeitet, informiert der Arbeitgeber den Betriebsrat (nach Anhang 3 Checkliste für Informationen zum System).
- **Rechtmäßigkeit**: Prüfung, ob eine rechtliche Grundlage für die Verarbeitung vorliegt.
- **Zweckbindung**: Prüfung, ob ein berechtigter Zweck für die Verarbeitung vorliegt. Der Zweck der geplanten Datenverarbeitung ist detailliert zu beschreiben. Unbestimmte und allgemeine Aussagen sind nicht zulässig.
- **Datenminimierung**: Prüfung, ob die Datenerhebung und -verarbeitung auf das notwendige Mindestmaß beschränkt wird. Von den Verantwortlichen ist zu prüfen, ob das angestrebte Ziel der Datenverarbeitung auch ohne Personenbezug mit vertretbarem Aufwand erreicht werden kann.
- **Richtigkeit:** Die verarbeiteten personenbezogenen Daten müssen immer aktuell und den tatsächlichen Gegebenheiten entsprechen.
- **Speicherbegrenzung**: Personenbezogene Daten von Beschäftigten dürfen nur so lange verarbeitet werden, bis der Zweck der Datenverarbeitung erfüllt ist. Für jedes System ist ein Löschkonzept vorzulegen.
- **Integrität und Vertraulichkeit:** Beschäftigtendaten sind vor unzulässigen oder unrechtmäßigen Kenntnisnahmen innerhalb und außerhalb des Betriebs oder Unternehmens zu schützen

5. Kategorisierung personenbezogener Daten nach verschiedenen Datenschutz- und Datensicherheitsniveaus

Die Datenkategorien, welche von Beschäftigten verarbeitet werden, sind für jedes eingesetzte IT-System anzugeben. Sensible Daten bzw. besondere Kategorien personenbezogener Daten nach Art 9 und 10 DSGVO (z.B.: Gesundheitsdaten, biometrische Daten, Gewerkschaftszugehörigkeit;) sind gesondert hervorzuheben. Die Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten ist nur zulässig,

- wenn es hierfür eine ausdrückliche und freiwillige Einwilligung der Beschäftigten gibt, die sich ausdrücklich auf diese Daten bezieht,

(Bei der Beurteilung, ob die für die Wirksamkeit einer Einwilligung notwendige Freiwilligkeit vorliegt, sind insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der Beschäftigten zu berücksichtigen sowie die Umstände, unter denen die Einwilligung erteilt worden ist).

- wenn es hierfür eine zwingende gesetzliche Voraussetzung gibt oder
- wenn die Verarbeitung im Rahmen des Ausnahmetatbestands in Art. 9 Abs. 2 lit d DSGVO durch eine dort genannte Stiftung, Vereinigung oder Organisation erfolgt.

Weiters ist die Verarbeitung für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen, Grundrechte und Grundfreiheiten der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen

IT-Systeme, die personenbezogene Daten besonderer Kategorie, Standortdaten oder Audio- und Bilddaten (Bsp. Überwachungskameras) verarbeiten oder Leistungs- und Verhaltenskontrollen zum Ziel haben, sind jedenfalls über eine Zusatzbetriebsvereinbarung zu regeln. Je nach System können aber auch andere Datenkategorien für Leistungs- und Verhaltenskontrollen verwendet werden (z.B. Geschäftsdaten, wenn der gesamte Arbeitsablauf aufgezeichnet wird, oder Protokolldaten, die das BenutzerInnenverhalten nachvollziehbar machen.), auch wenn dies nicht auf den ersten Blick sichtbar ist. In diesem Fall ist ebenfalls eine Zusatzbetriebsvereinbarung abzuschließen.

6. Betriebliche Personaldatenschutzkommission (PDSK)

Zur Beratung aller Fragen, die sich im Zusammenhang mit der Einführung, dem Betrieb, der Auslegung und den Änderungen von IT-Systemen ergeben, wird eine innerbetriebliche Personaldatenschutzkommission (PDSK) gebildet. Die Beratungen, Ergebnisse und Erkenntnisse der PDSK dienen der Unternehmensleitung und dem Betriebsrat als Entscheidungsgrundlagen.

Die Entscheidungskompetenzen der Unternehmensleitung als Organ des Unternehmens und die des Betriebsrates als Körperschaft gemäß ArbVG bleiben davon unberührt.

6.1. Zusammensetzung

Dieser Kommission gehören paritätisch an [je nach Unternehmensgröße]:

- zwei - vier von der Unternehmensleitung nominierte VertreterInnen
- zwei - vier vom Betriebsrat nominierte VertreterInnen
- so vorhanden: der betriebliche Datenschutzbeauftragte (DSB)

Unternehmensleitung und Betriebsrat haben jeweils das Recht, bei Bedarf Fachpersonal ihrer Wahl zur Beratung beizuziehen. Eventuell anfallende Kosten sind vom Unternehmen zu tragen.

Die Tätigkeit der PDSK-Mitglieder erfolgt während der bezahlten Arbeitszeit und ihnen dürfen aus dieser Tätigkeit keine Nachteile entstehen.

Die PDSK legt eine Geschäftsordnung fest.[2]

6.2. Aufgaben der PDSK

Aufgabe der PDSK ist es, einen Interessenausgleich zwischen Unternehmensleitung und Betriebsrat herbeizuführen. Auch eine Nichteinigung im Zusammenhang mit dieser Betriebsvereinbarung ist in der PDSK zu behandeln. Die PDSK schlägt vor, wie die personenbezogenen Daten von Beschäftigten in Anlehnung an Pkt. 5 dieser Vereinbarung kategorisiert werden. Sie schlägt geeignete technische und organisatorische Maßnahmen vor, um die Einhaltung dieser Betriebsvereinbarung sowie der jeweils geltenden gesetzlichen Bestimmungen zu überprüfen und sicherzustellen. Besteht keine PDSK, sind die Aufgaben vom Betriebsrat so weit wie möglich zu übernehmen.

Die Tätigkeit der PDSK ist nicht mit einer Schlichtungsstelle gleichzusetzen, die Rechte des Betriebsrats auf Anrufen der gerichtlichen Schlichtungsstelle bleiben durch die Errichtung und Tätigkeit der PDSK unberührt.

[2] Ein Muster für eine Geschäftsordnung ist in der GPA erhältlich

7. Grundsätzliche Anforderungen bei der Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis

7.1. Umgang mit Log- und Protokolldaten

Log- und Protokolldaten, die je nach System BenutzerInnenaktivitäten dokumentieren, dürfen nur zu folgenden Zwecken verwendet werden:

- Einhaltung von Maßnahmen zur Datensicherheit (Art 5 Abs 1 lit f DSGVO)
- Überprüfung der Einhaltung von Betriebsvereinbarungen,
- Gewährleistung der Systemsicherheit,
- Analyse und Korrektur von technischen Fehlern im IT-System,
- Optimierung des Computersystems,
- Leistungsverrechnung für den Betrieb der Hardware, Software und Netzwerkserver.

Stufenweise Kontrollverdichtung

Grundsätzlich wird die Protokollierung von Daten aus technischen Gründen maschinen- und damit auch personenbezogen vorgenommen. Der direkte Personenbezug wird aber nur unter bestimmten Bedingungen einer bestimmten Personengruppe zugänglich gemacht. Die Analyse dieser Daten findet grundsätzlich im Sinne einer stufenweisen Kontrollverdichtung statt:

Stufe 1: Die Kontrolle erfolgt vorerst nur durch die IT-Abteilung und ohne konkreten Personenbezug. Bei signifikanten Auffälligkeiten (z.B. Zugriffsstatistiken, Downloadvolumen) wird der betroffene Personenkreis über geltende betriebliche Regelungen informiert und zur Verhaltensänderung aufgefordert.

Stufe 2: Im Fall des Weiterbestehens einer Gefahr für die betriebliche IT-Infrastruktur (z. B. Virenattacke) oder einer hohen Wahrscheinlichkeit, dass tatsächlicher Schaden für die Firma entstehen wird (z. B. Datenverlust), ist die/der einzelne Betroffene zu informieren.

Stufe 3: Erst bei fortgesetzter pflichtwidriger und System gefährdender Nutzung kann die Offenlegung der personenbezogenen Daten gegenüber der vorgesetzten Person unter Hinzuziehung des Betriebsrates erfolgen.

Zugriffe durch die IT-Abteilungen sind zu protokollieren, damit tatsächlich durchgeführte Verarbeitungsvorgänge im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Weiters ist der Prozess der stufenweisen Kontrollverdichtung zu protokollieren, ebenso wie begründete Verdachtsmomente schriftlich festzuhalten sind.

Wird jemand unbegründet verdächtigt, sind die Protokolle sofort zu löschen, erhärten sich Verdachtsmomente, sind die Protokolle maximal drei Jahre nach dem ersten Verdachtsmomentzeitpunkt aufzubewahren. Ausgenommen von den ersten beiden Stufen der Kontrollverdichtung sind nur die Fälle

einer konkreten unmittelbaren Gefährdung für die IT-Infrastruktur oder ihre korrekte Funktionsfähigkeit. Darüber hinaus für all diejenigen Fälle, in denen ein begründeter Verdacht eines Verstoßes gegen strafrechtliche Bestimmungen vorliegt, der durch rasches Eingreifen vermieden werden kann.

7.2. Cloud Umgebungen und Software as a Service

Müssen Beschäftigte für die Erbringung ihrer vertraglich geschuldeten Tätigkeiten oder Aufgaben Software-Anwendungen nutzen, die eine personenbezogene Anmeldung erforderlich machen und werden dabei Beschäftigtendaten außerhalb des Betriebs in Cloud Umgebungen oder per „Software as a Service“ verarbeitet, dürfen nur die personenbezogenen Daten verwendet werden, die für den Anmeldeprozess zwingend erforderlich sind. Die Verarbeitung dieser Beschäftigtendaten muss sich auf die Prüfung der Nutzungs- und Zugriffsberechtigung der einzelnen Beschäftigten beschränken. Die Einhaltung dieser Vorgabe muss der Arbeitgeber sicherstellen.

Eine Übermittlung von Beschäftigtendaten aus Cloud-Umgebungen oder aus „Software as a Service“-Anwendungen in oder aus anderen betrieblichen Systemen ist nur zulässig, wenn diese unter Beachtung einschlägiger datenschutz- und arbeitsrechtlicher Vorgaben eingeführt worden sind.

7.3. Einsatz von Big Data Systemen und Algorithmen bzw. lernender Software (sog. Künstliche Intelligenz, KI)

Sollen Beschäftigtendaten aus verschiedenen Quell-Systemen auf Datenplattformen bzw. Data Warehouse-Lösungen (Big Data Systeme) zusammengeführt werden, ist darüber eine Zusatz-Betriebsvereinbarung abzuschließen. Der Einsatz solcher Systeme sollte auf die Bereitstellung statistisch relevanter Daten beschränkt werden.

Kommen im Betrieb Reporting-Tools wie Power BI zum Einsatz, bei denen User selbständig Auswertungen aus Datensätzen aus Data Warehouse Lösungen nach einem Baukastensystem erstellen können, so sind die Zugriffsrechte auf personenbezogene Datenkategorien für einzelne Benutzergruppen genau zu prüfen und in einer Zusatz-BV zu regeln.

Sollen personenbezogene Beschäftigtendaten mittels Algorithmeneinsatz bzw. KI-Anwendungen verarbeitet werden (z.B.: automatisches Monitoring bzw. Leistungs- und Verhaltenskontrolle, automatisches Auftragsmanagement, Kundenfeedback- und Leistungsbewertungssysteme;), sind Betriebsrat sowie die betroffenen ArbeitnehmerInnen vor dem Einsatz dieser Instrumente genau zu informieren und zu beteiligen. (Vgl. dazu Anhang 4 „Prüfkriterien zum Erkennen einer KI-Anwendung.)

Die Schaffung von Transparenz und Nachvollziehbarkeit sowie Verständlichkeit ist die Grundvoraussetzung für den Einsatz von Algorithmischem Management bzw. Künstlicher Intelligenz im Beschäftigungsverhältnis. In der Regel ist für solche Anwendungen eine Datenschutzfolgenabschätzung und die Zustimmung des Betriebsrates erforderlich.

Automatisierte Entscheidungen im Einzelfall und Profiling sind im Beschäftigtenverhältnis untersagt.

7.4. Simulationsdaten (Testdaten)

Bei der Entwicklung und Erweiterung von IT-Systemen muss mit Simulationsdaten (Testdaten) gearbeitet werden. Falls eine Anonymisierung oder Pseudonymisierung nicht möglich ist, werden Echtdaten verwendet und es gelten die Regelungen dieser Rahmenvereinbarung bzw. der jeweiligen Einzelvereinbarung.

7.5. Benutzerservice / Auskunftsperson / Helpdesk

Hard- und Software der IT-Systeme werden durch ein Benutzerservice betreut. Es ist sicherzustellen, dass für Beschäftigte an Bildschirmarbeitsplätzen AnsprechpartnerInnen zur Verfügung stehen.

Sollte eine Hilfestellung durch Aufschalten in die aktuelle Arbeitsumgebung erfolgen, ist dies nur nach Aufforderung durch die Betroffenen und deren Zustimmung für jeden einzelnen Fall erlaubt. Der Ferneinstieg des Systembetreuers / der Systembetreuerin in eine fremde Anwendung, ist durch ein optisches Signal zu kennzeichnen. Der Ausstieg des Systembetreuers/ der Systembetreuerin nach erfolgter Hilfestellung wird ebenfalls auf dem Bildschirm angezeigt.

Eine Auswertung, welche Beschäftigten zu welchem Zeitpunkt das Help-Desk-System in Anspruch genommen haben, findet nicht statt. Es wird lediglich anonym die Art der Hilfestellung dokumentiert, um Hinweise für zukünftige Schulungsinhalte zu bekommen.

7.6. Datenverarbeitung durch integrierte Endgeräte

Beschäftigtendaten, die von in Geräten oder Arbeitsmitteln integrierten IT-Anwendungen erhoben und verarbeitet werden, die ihrerseits mit betrieblichen Systemen in Verbindung stehen, dürfen nicht für Verhaltens- oder Leistungskontrollen der Beschäftigten verwendet werden, die mit diesen Geräten arbeiten. Deshalb ist die Herstellung eines Personenbezugs zwischen den Daten in Geräten oder Arbeitsmitteln und Beschäftigten unzulässig. Diese Vorgabe ist durch eine durchgängige und automatisierte Anonymisierung der vorhandenen Daten zu erreichen. Wo diese technisch unmöglich ist, sind Löschverfahren zu verankern, durch die die in Geräten oder Arbeitsmitteln erzeugten Daten bei einer weiteren Verarbeitung kurzfristig überschrieben werden.

Müssen Geräte und Arbeitsmittel mit integrierten IT-Anwendungen aus betrieblichen Gründen von Beschäftigten permanent getragen oder mitgeführt werden, muss es den Beschäftigten möglich sein, die stattfindende Datenverarbeitung aus persönlichen Gründen jederzeit auf einfache Art und Weise zu unterbrechen. Die Unterbrechung der Datenerfassung und Verarbeitung darf nur durch ein aktives Handeln der Beschäftigten wieder aufgehoben werden können.

Eine Unterbrechung der Datenverarbeitung darf für Beschäftigte nicht zu arbeitsrechtlichen Nachteilen führen.

7.7. Biometrische Kontrollverfahren

Die Verarbeitung biometrischer Daten von Beschäftigten ist unzulässig.

Abweichend davon ist die Verarbeitung biometrischer Daten von Beschäftigten ausnahmsweise zulässig, wenn nur so unumgängliche technische und organisatorische Sicherheitsmaßnahmen realisiert werden können und keine alternativen Methoden möglich sind. Zudem muss der mit der Verarbeitung angestrebte Zweck von Arbeitgebern transparent, klar und abschließend festgelegt sein. Verarbeitungen biometrischer Beschäftigtendaten für andere Zwecke sind ausgeschlossen.

7.8. Auftragsverarbeitung

Der Verantwortliche hat mit jedem Auftragsverarbeiter eine Vereinbarung zu treffen und auf die Regelungen dieser Betriebsvereinbarung und der betreffenden Zusatzvereinbarung nachweislich hinzuweisen. Der Auftragsverarbeiter gibt die Regelungen der Betriebsvereinbarung auch an etwaige Sub-Auftragsverarbeiter weiter. Dem Betriebsrat ist eine Kopie der jeweiligen Verträge zur Verfügung zu stellen.

7.9. Beweisverwertungsverzicht

Die Geschäftsführung verzichtet ausdrücklich darauf, Informationen, die unter Verletzung der Bestimmungen dieser Betriebsvereinbarung oder durch Zufallsfunde gewonnen wurden, als Beweismittel zur Begründung arbeitsrechtlicher Maßnahmen zu verwenden.

7.10. Schulung von AdministratorInnen

(System-)AdministratorInnen sind über Datenschutzrecht sowie die Bestimmungen dieser BV und der für sie relevanten Zusatz-BVs zu schulen.

8. Rechte des Betriebsrates

8.1. Informationspflichten des Unternehmens

Das Unternehmen verpflichtet sich, dem Betriebsrat zu jenen Datenverarbeitungen, in denen personenbezogene Beschäftigtendaten verwendet werden, alle wesentlichen Informationen (laut Anhang 3) zur Verfügung zu stellen.

8.2. Informationsrechte des Betriebsrates

Für zukünftige (geplante) IT-Systeme und Verwendungen sind zusätzlich folgende Informationen zur Verfügung zu stellen:

- geplante Auswirkungen des Projektes (z. B. Personalausmaß, Veränderung von Arbeitsabläufen)
- den Zeitplan des Projektablaufes bis zur Umsetzung
- Bekanntgabe der ProjektleiterInnen, System-Verantwortlichen und etwaiger TeilprojektleiterInnen
- Bekanntgabe eventueller externer BeraterInnen und Firmen

- Gesamtkosten des Projektes

Sofern ein IT-System die Verwendung von personenbezogenen Beschäftigtendaten möglich macht, ist bereits in der Planungsphase, d.h. vor Einführung bzw. Veränderung des IT-Systems die PDSK und der Betriebsrat einzubinden. Diese Systemänderungen oder -entwicklungen sind vor ihrer Implementierung zu dokumentieren und der PDSK zur Verfügung zu stellen.

8.3. Anhörungs- und Mitwirkungsrecht des Betriebsrates nach Art 35 Abs 9 DSGVO

Vor dem Einsatz einer neuen Datenverarbeitung muss geprüft werden, ob ein hohes Risiko für die Grundrechte der betroffenen ArbeitnehmerInnen besteht und daher eine Datenschutz-Folgenabschätzung laut Art 35 DSGVO erforderlich ist (Schwellenwertanalyse). Dazu holt der Arbeitgeber die Stellungnahme des Betriebsrates laut Art 35 Abs 9 DSGVO ein und berücksichtigt diese. Anschließend wird gemeinsam dokumentiert, ob eine Datenschutz-Folgenabschätzung durchgeführt wird oder nicht und warum. Über Maßnahmen zur Senkung des Risikos für die Rechte und Freiheiten der betroffenen ArbeitnehmerInnen wird mit dem Betriebsrat beraten und – wenn nötig – eine Betriebsvereinbarung abgeschlossen.

8.4. Kontrollrechte des Betriebsrates

Der Betriebsrat hat das Recht, in sämtliche Protokolle und Auswertungen Einsicht zu nehmen bzw. solche anzufordern. [Ausnahme: Die Einsicht in einen Personalakt bedarf der Zustimmung des/der betroffenen Beschäftigten.]

Dem Betriebsrat sind neben der entsprechende Hard- und Software Zugriffsberechtigungen (Leseberechtigungen) zur Verfügung zu stellen, die ihm die Kontrolle der IT-Systemen ermöglichen.

Es steht dem Betriebsrat zu, externe ExpertInnen hinzuzuziehen. Diese ExpertInnen sind zur Verschwiegenheit verpflichtet. Sie sind von den zuständigen Fachabteilungen zu unterstützen. Das Unternehmen trägt die anfallenden Kosten (Sacherfordernisse nach § 72 ArbVG).

8.5. Besonderes Schulungsrecht des Betriebsrates

Die Mitglieder des Betriebsrates haben unter Fortzahlung des Entgeltes das Recht, sowohl innerbetriebliche als auch außerbetriebliche einschlägige Fort- und Weiterbildungsangebote in Anspruch zu nehmen und die Kosten trägt der/die ArbeitgeberIn.

Es wird vereinbart, dass die Ausübung des besonderen Schulungsrechts nicht auf einen Anspruch gemäß § 118 ArbVG angerechnet wird.

9. Rechte der Beschäftigten

9.1. Vorgangsweise bei Verdacht auf unzulässige Datenverwendung

Klargestellt wird: Verstößt eine Weisung hinsichtlich der Zulässigkeit einer Verarbeitung oder Übermittlung gegen höherrangige Bestimmungen (insb. DSGVO und Datenschutzgesetz), so ist sie nichtig und muss nicht befolgt werden. Sind Beschäftigte über die Zulässigkeit einer Verarbeitung oder Übermittlung im Zweifel, sind sie berechtigt, die erteilte Weisung zu dokumentieren oder in einer „Bestätigung“ an ihren Vorgesetzten zu verschriftlichen.

9.2. Beschäftigte bzw. Familienangehörige als Kunden (Trennungsgebot)

Für den Fall, dass im Unternehmen Daten von Beschäftigten bzw. ihrer Familienangehörigen als PatientInnen, KlientInnen oder KundInnen vorliegen, ist eine Verknüpfung dieser Daten mit den Beschäftigtendaten grundsätzlich untersagt. Der Zugriff auf diese Kundendaten muss restriktiv geregelt werden. Ausnahmen sind nur im Einvernehmen mit den Beschäftigten und ihren Familienangehörigen unter Einbeziehung des Betriebsrates zulässig.

9.3. Privatnutzung

Die Nutzung der betrieblichen IT-Systeme für private Zwecke ist in angemessenem Ausmaß zulässig. Es können alle Beschäftigten auf ihren Laufwerken bzw. im verwendeten Kommunikationssystem einen Ordner "privat" anlegen, dessen Inhalt keinesfalls von dritter Seite ohne Zustimmung der Betroffenen eingesehen oder ausgewertet werden darf.

Die ArbeitnehmerInnen haben dabei jedoch betriebliche Regelungen im Hinblick auf Daten- und Netzwerksicherheit zu berücksichtigen, die den uneingeschränkten Gebrauch von Daten unterbinden (z.B. Downloads aus dem Internet, Installieren neuer Software).

10. Bestehende und neue IT-Systeme

Es wird einvernehmlich als Ziel festgehalten, für alle IT-Systeme, die personenbezogene Beschäftigtendaten verwenden, eine datenschutz- und arbeitsrechtlich konforme Grundlage zu schaffen. Daher ist der Betriebsrat über alle zum Zeitpunkt des Abschlusses dieser Rahmenbetriebsvereinbarung bestehenden und nicht mit Betriebsvereinbarung geregelten IT-Systeme, die personenbezogene Daten verarbeiten, zu informieren. Diese haben das in der Rahmenbetriebsvereinbarung beschriebene Prozedere

zu durchlaufen, d.h. sie sind in den Anhängen zu dokumentieren, und je System ist ein Datenblatt bzw. bei Bedarf eine Zusatzbetriebsvereinbarung abzuschließen.

In den Zusatzvereinbarungen sind je IT-System die Informationen laut Anhang 3 anzuführen. Sollten angeführte Informationen nicht zur Verfügung stehen, ist der Grund zu dokumentieren.

11. Inkrafttreten und Vertragsdauer

Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft und gilt unbefristet.

Sie kann jedoch bei Übereinstimmung zwischen ArbeitgeberIn und Betriebsrat, jederzeit ergänzt werden.

Zeichnungsbevollmächtigte

für das Unternehmen

für den Betriebsrat

ANHANG 1: IT-Systeme, deren Verarbeitung personenbezogener Daten von Beschäftigten durch diese Rahmenbetriebsvereinbarung abschließend gedeckt sind

Bezeichnung System	Aufnahmedatum	Anmerkungen

Datenblatt pro System - Mindestinhalte

	Dokumentation
Bezeichnung IT-System	
Zweck der Datenverarbeitung	
personenbezogene Datenkategorien	
vereinbarte personenbezogene Auswertungen und Analysen	
Übermittlung der erzeugten Daten in andere Systeme (Beschreibung Schnittstelle)	
Übermittlung von Daten an betriebsexterne Empfänger	
Rollen- und Berechtigungskonzept	
(optional) organisatorische Regeln	
Datum/Versionsnummer	
Unterschrift Arbeitgeber/Betriebsrat	

ANHANG 2: bestehende Betriebsvereinbarungen zu IT-Systemen

Bezeichnung System	Datum Betriebsvereinbarung	Anmerkungen

ANHANG 3: Information zu IT-Systemen

Je Informations- und Kommunikationssystem (IKT-System) sind folgende Informationen zur Verfügung zu stellen:

- Name des IT-Systems (Datenanwendung), Versionsbezeichnung und Anbieter
- die jeweiligen Systembeschreibungen / Benutzerhandbücher
- betriebliche(r) Verantwortliche(r) / Ansprechperson(en)
- Vollständige und aktuelle Dokumentation aus dem Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO mit allen dort angeführten Punkten
    - Zweck der Verarbeitung
    - Betroffenenkategorien und die dazu jeweilig verarbeiteten Datenkategorien
    - Empfänger (samt (Sub-) Auftragsverarbeiter) von personenbezogenen Daten
    - Bei Übermittlung von personenbezogenen Daten in ein Drittland, die Angabe des Drittlandes und geeignete Garantien für die Datenübermittlung
    - Lösch- und Aufbewahrungsfristen
    - Beschreibung der Technisch-Organisatorischen Maßnahmen zur Sicherheit der jeweiligen Datenverarbeitung (Art 32 DSGVO)
- Rechtsgrundlage der Datenverarbeitung
- Mandanten, die personenbezogene Echtdaten verwenden (z.B. Testsystem, Konsolidierungssystem, Produktivsystem)
- eingesetzte Systemteile / Module
- Standort und Art der Datenerfassungsgeräte (z. B. Terminals, Kameras, Automaten, …)
- ein Verzeichnis personenbezogener Auswertungen mit Beispielen
- Schnittstellen (Import und Export) zu anderen IT-Systemen
- Zugriffsberechtigungsverzeichnis und mögliche Empfängerkreise
- Die Ergebnisse der allfällig durchgeführten Datenschutz-Folgenabschätzung bzw. die Dokumentation der Schwellwertanalyse, wenn keine Datenschutz-Folgenabschätzung durchgeführt wurde
- Auflistung allfällig eingeführter Verfahrensregeln und Zertifizierungen
- Form der Protokollierung

ANHANG 4: Prüfkriterien zum Erkennen einer KI-Anwendung

KI-Anwendungen werden in der Regel als Teil eines größeren IT-Systems eingesetzt. Folgende Fragen sollen helfen, KI-Funktionen zu erkennen.

- Werden im großen Maßstab detaillierte Daten von (verschiedenen) IT-Systemen erfasst und mithilfe neuer digitaler Technologien verarbeitet („Big Data“)?
- Wird oder wurde das System mittels Daten trainiert?
- Wird komplexes Erfahrungs- und Prozesswissen der MitarbeiterInnen erhoben und systematisch in IT-Systeme überführt?
- Findet mit dem neuen System automatisiert eine Profilbildung oder Klassifizierung von Beschäftigten(-gruppen) statt? („People Analytics“)
- Verarbeitet das System natürliche Sprache (durch z.B.: automatische Verschriftlichung, Vorlesen, Übersetzen;)?
- Verarbeitet das System selbständig Bilddaten und kann es darauf komplexe Muster (Gesichter, fehlerhafte Produkte?) erkennen?
- Kann man sich mit dem System unterhalten (Chat-Bot)?
- Ist das System für vorausschauende Vorhersagen („predictive analytics“) zu verwenden? (z.B. Austrittswahrscheinlichkeit von Beschäftigten)

Lautet die Antwort auf eine oder mehrere Fragen „Ja“, werden mit großer Wahrscheinlichkeit Komponenten von KI eingesetzt.

In diesem Fall hat der Arbeitgeber dem Betriebsrat detaillierte Informationen zu dieser KI-Anwendung vorzulegen (z.B. laut KI-Frageliste der GPA), um eine Risikobewertung durchführen zu können. Dabei sind Auswirkungen auf Bereiche wie potentielle Leistungs- und Verhaltenskontrolle, Beschäftigtendatenschutz, Arbeitsbedingungen (Arbeitsplatzeinsparung, Entscheidungsspielräume, Abwechslungsreichtum, Leistungsdruck, usw.) zu beachten.

Je nach Ergebnis der Risikobewertung ist der Regulierungsbedarf für die jeweilige KI-Anwendung zu bestimmen.