Vorbemerkung zu Aufbau und Unterscheidung Rahmenbetriebsvereinbarung und Zusatz-Betriebsvereinbarung(en)

Hintergrund: 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.

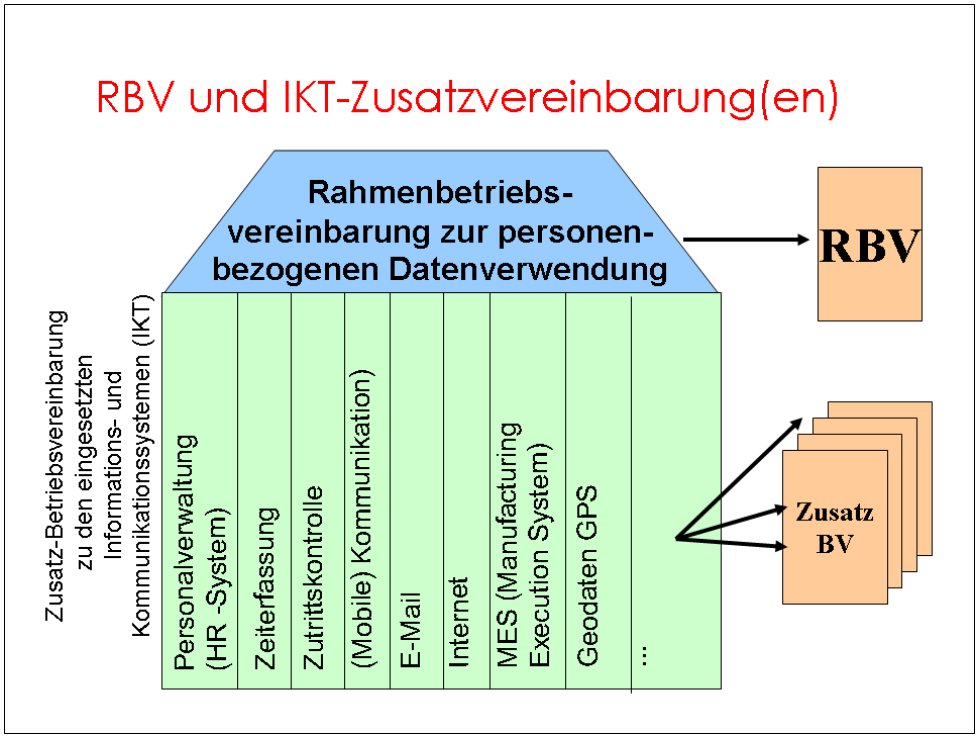
Viele dieser Betriebsvereinbarungen beinhalten Regelungen, die unabhängig vom eingesetzten Informations- und Kommunikationssystem (IKT) sind. Darunter fallen z.B. die allgemeinen Mitgestaltungs- und Kontrollrechte des Betriebsrates, die Informationsrechte der Beschäftigten nach Datenschutzgesetz, unternehmensweite Regelungen zur Einhaltung des Datenschutzes, usw.

Aufgrund der technologischen Schnelllebigkeit und häufiger Veränderungen in der Funktionalität der eingesetzten IKT, erscheint es sinnvoll, ein abgestuftes Konzept anzuwenden, das diesem technischen Fortschritt entgegenkommt, ohne rechtliche Anforderungen zu untergraben.

Daher empfiehlt die GPA-djp die Teilung in eine übergreifende, allgemein gültige Rahmenbetriebsvereinbarung (RBV) zur Verwendung personenbezogener Daten im Betrieb und Zusatzbetriebsvereinbarungen zu den konkreten im Einsatz befindlichen bzw. geplanten IKT.

Dabei sind in der Rahmenbetriebsvereinbarung sämtliche organisatorische, systemunabhängige Regelungen (betriebliche „Spielregeln") zu finden, wohingegen in den Zusatzbetriebsvereinbarungen die konkreten Systeme bzw. Anwendungen (z.B. Zeiterfassung, Zutrittskontrolle, Telefonsystem, Internetgebrauch,...) geregelt werden. Dazu zählen auch die technischen Details (somit der IST-Stand), die mitunter auch in Form von Anhängen dargestellt werden.

Die folgende Abbildung dokumentiert diese Unterteilung.



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 möglichst optimal passende Vereinbarung zu entwickeln. Die GPA-djp unterstützt und berät Sie gerne auf diesem Weg!

Hinweis: Die in der Muster-Betriebsvereinbarung grau hinterlegten Passagen sind als Kommentare zu verstehen und stellen keinen normativen Betriebsvereinbarungstext dar.

RAHMENBETRIEBSVEREINBARUNG
über die Verwendung personenbezogener Beschäftigtendaten

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] andererseits

1) GELTUNGSBEREICH

Diese Betriebsvereinbarung gilt:

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

Sachlich: allgemeine organisatorische Regelungen für die Planung, Einführung, Verwendung und Veränderung bestehender und zukünftiger Informations- und Kommunikationssysteme (IKT-Systeme), die personenbezogene Daten von Beschäftigten verwenden.

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

2) RECHTSGRUNDLAGEN UND BEGRIFFSDEFINITIONEN

Die rechtliche Basis bilden insbesondere

- die Bestimmungen des Arbeitsverfassungsgesetzes (ArbVG) im Besonderen die §§ 89, 91, 92, 96, 96a und 97
- die Bestimmungen der EU-Datenschutzgrundverordnung und des Datenschutzanpassungsgesetzes 2018
- die Bestimmungen des ArbeitnehmerInnenschutzgesetzes (ASchG) [im Zusammenhang mit IKT-Einsatz ist insbesondere § 68 zur benutzergerechten Gestaltung von Bildschirmarbeitsplätzen wichtig, wobei auch die Bildschirme von diversen mobilen Geräten gemeint sind]
- das Kommunikationsgeheimnis nach § 93 Abs 3 Telekommunikationsgesetz (TKG)

Die Definitionen aus der Europäischen Datenschutzgrundverordnung (DSGVO) und des Datenschutzanpassungsgesetzes 2018 (DSAG) finden in dieser Betriebsvereinbarung Anwendung.

3) ZIELSETZUNG

Diese Betriebsvereinbarung dient zur rechtlichen Qualitätssicherung und Transparenz bei der Verwendung personenbezogener Daten beim Einsatz von Informations- und Kommunikationssystemen (IKT-Systemen). Sie kann Betriebsvereinbarungen zu einzelnen IKT-Systemen nicht ersetzen, gibt aber einen Rahmen vor. Personenbezogene Daten von Beschäftigten dürfen nur verwendet werden, soweit der Verwendungszweck rechtlich gedeckt ist. [Falls innerbetriebliche Verhaltensrichtlinien (z.B. Governance und Compliance) vorhanden sind, empfiehlt es sich, diese im Hinblick auf die nationalen Gesetze und diese Rahmenbetriebsvereinbarung zu überprüfen und miteinander in Einklang zu bringen.]

Daher sind bei jeder IKT, die personenbezogene Beschäftigtendaten verwendet, folgende Prüfungsmaßstäbe (in dieser Reihenfolge) anzuwenden:

a) Prüfung, ob eine rechtliche Grundlage nach Art 5 Abs 1 lit a DSGVO vorliegt.

b) Prüfung, ob ein berechtigter Zweck nach Art 5 Abs 1 lit b DSGVO vorliegt. Der Zweck der geplanten Datenverarbeitung ist detailliert zu beschreiben. Unbestimmte und allgemeine Aussagen sind nicht zulässig.

c) Prüfung, ob die Datenerhebung und -verarbeitung auf das notwendige Mindestmaß beschränkt wird (Art 5 Abs 1 lit c DSGVO). Dazu sind Maßnahmen im Sinne der Modelle „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen" (Art 25 DSGVO) zu setzen.

Bereits bei Planung und Einführung der IT-Systeme wird dokumentiert, wie die Datenschutzgrundsätze eingehalten werden (Rechenschaftspflicht Art 5 Abs 2 DSGVO).

4) UMGANG MIT PERSONENBEZOGENEN DATEN

Daten über Benutzeraktivitäten dürfen nur zu folgenden Zwecken verwendet werden:

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

Protokolldaten dürfen ausschließlich dahingehend geprüft werden, ob die Zugriffsberechtigungen vorhanden waren. Eine Auswertung der Protokolle im Hinblick auf das Benutzerverhalten einzelner Personen ist jedenfalls rechtlich unzulässig (Art 5 Abs 1 lit f, 25, 30 Abs 1 lit f, 40 ff iVm Art 12-14 DSGVO). Die Geschäftsführung verzichtet ausdrücklich darauf, Informationen, die unter Verletzung der Bestimmungen dieser Betriebsvereinbarung gewonnen wurden, als Beweismittel zur Begründung arbeitsrechtlicher Maßnahmen zu verwenden.

4.1 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.

Stufe 1: Die Kontrolle erfolgt allerdings im Sinne einer *stufenweisen Kontrollverdichtung* vorerst nur durch die IT-Abteilung und ohne konkreten Personenbezug.

Stufe 1a: Sollte sich das auftretende Problem nicht rein technisch lösen lassen, wird der betroffene Personenkreis (z.B. Abteilung, Team, Bürobereich,…) informiert und zur Verhaltensänderung aufgefordert.

Stufe 2: Im Fall des Weiterbestehens einer Gefahr für die betriebliche IKT-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 Hinzuziehen des Betriebsrates erfolgen.

Der Prozess der stufenweisen Kontrollverdichtung ist zu protokollieren, ebenso wie begründete Verdachtsmomente schriftlich festzuhalten sind. Wird jemand zu Unrecht verdächtigt, sind die Protokolle sofort zu löschen, erhärten sich Verdachtsmomente sind die Protokolle maximal drei Jahre nach dem ersten Verdachtsmomentzeitpunkt aufzubewahren (Art 10 ff DSGVO). Ausgenommen von den ersten beiden Stufen der Kontrollverdichtung sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IKT-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.

4.2 Kategorisierung personenbezogener Daten nach verschiedenen Datenschutz- und Datensicherheitsniveaus

Es ist eine Differenzierung nach Datenarten/-kategorien vorzunehmen (Art 9, 10), um die erhöhten Schutzanforderungen für die Verarbeitung besonderer Datenkategorien (ethnische Herkunft, politische Meinung, Religion, sexuelle Orientierung, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Daten über Verurteilungen und Straftaten) zu gewährleisten.

ACHTUNG: Nach Vorstrafen und laufenden Ermittlungsverfahren darf der Arbeitgeber idR gar nicht fragen, geschweige denn darf er solche Daten speichern. Ausnahme: Wenn zwischen dem Tätigkeitsbereich des Arbeitnehmers und einem begangenen Delikt ein Zusammenhang besteht (z.B. KassierIn in einem Geldinstitut und Vermögensdelikte; LehrerInnen und Kindesmissbrauchsdelikte).

[Die folgende Einstufung ist eine wichtige Grundlage für das Verarbeitungsverzeichnis, die interne Dokumentation der Datenanwendungen (Art 30 DSGVO), für eine allfällige Datenschutz-folgeabschätzung (Art 35 DSGVO) und für die Frage, bei welchen Systemen eine Mitbestimmung nach ArbVG vorliegt (manchmal B, immer C und D).]

Die Datenkategorisierung erfolgt nach der in Anhang 2 beschriebenen Vorgangsweise.

5) BETRIEBLICHE PERSONALDATENSCHUTZKOMMISSION (PDSK)

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

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

5.1 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 bei zu ziehen.

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

Die PDSK legt eine Geschäftsordnung nach dem Muster im Anhang 3 fest.

5.2 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 in Anlehnung an Pkt. 4.2 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.

Alle zum Zeitpunkt des Abschlusses dieser Rahmenbetriebsvereinbarung bestehenden und nicht mit Betriebsvereinbarung geregelten IKT-Systeme, die personenbezogene Daten verwenden, sind der PDSK unter Angabe der in Anhang 1 beschriebenen Informationen umgehend zu melden und haben das folgende Prozedere zu durchlaufen.

In der PDSK ist für jedes IKT-System zu klären, bei welchen Daten ein Personenbezug im Sinne der Bestimmungen des Art 4 DSGVO vorliegt (z.B. durch Kostenstellennummer o.ä.).

Von den Systemverantwortlichen ist zu prüfen, ob das angestrebte Ziel der Datenverwendung auch ohne Personenbezug mit vertretbarem Aufwand erreicht werden kann.

Ist dies nicht der Fall, überprüft die PDSK die Notwendigkeit des Abschlusses einer Zusatzbetriebsvereinbarung für das konkrete IKT-System im Sinne der §§ 96, 96a bzw. 97 ArbVG.

Die PDSK schlägt bei Einführung neuer IKT-Systeme Maßnahmen vor, die Datensparsamkeit durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art 25 DSGVO) garantieren.

Weiters prüft die PDSK, ob eine geplante Datenverarbeitung für die Betroffenen risikoreich ist und eine Datenschutz-Folgenabschätzung nach Art 35 DSGVO erforderlich ist. Ist das der Fall, wird eine DS-Folgenabschätzung durchgeführt und allfällige Maßnahmen zur Eindämmung des Risikos in der PDSK erarbeitet, dabei werden schriftliche Empfehlungen der Aufsichtsbehörde einbezogen.

Die gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten nach Art 37 DSGVO wird von der PDSK geprüft.

Die PDSK entwickelt gemeinsam mit dem Datenschutzbeauftragten, der Unternehmensleitung und dem Betriebsrat ein Datenschutzkonzept und erstellt einmal jährlich einen Datenschutzreport. Dieser Datenschutzreport dient der Unternehmensleitung und dem Betriebsrat zur Diskussion, Evaluation und Weiterentwicklung der bestehenden Betriebsvereinbarungen. In diesem Datenschutzreport werden die wesentlichen Problembereiche betreffend Datensicherheit und Datenschutz dargestellt, wobei auch die Anwendbarkeit und die mögliche Ergänzung der bestehenden Betriebsvereinbarungen untersucht werden.

6) MASSNAHMEN BEI DER VERWENDUNG PERSONENBEZOGENER DATEN

6.1 Übertragung von Daten auf PCs, Laptops, mobile Geräte oder dgl.

Bei der Übertragung von personenbezogenen Daten auf Personal Computer (PC), Laptop, mobile Geräte (z.B.: Smartphone, Tablet-PC, USB-Stick, externe Festplatten) oder dgl. gilt im Hinblick auf alle Daten eine besondere Sorgfaltspflicht. Für die Verarbeitung besonderer Kategorien personenbezogener Daten ist für jedes System eine Regelung in der Zusatzvereinbarung zu treffen.

6.2 Aufbewahren und Löschen personenbezogener Daten

Für alle personenbezogenen Daten ist in der jeweiligen Zusatzvereinbarung eine Frist zu vereinbaren, bis wann diese Daten zu löschen sind. Die Löschung ist vorzunehmen, wenn die Datenverwendung ihren Zweck erfüllt hat.

6.3 Simulationsdaten (Testdaten)

Bei der Entwicklung und Erweiterung von IKT-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.

6.4 Auftragsverarbeiter

Alle zum Einsatz kommenden Auftragsverarbeiter müssen eine ausreichende Gewähr für die rechtmäßige und sichere Datenverwendung im Sinne des Art 28 DSGVO bieten.

Der Verantwortliche hat dazu mit jedem Auftragsverarbeiter eine Vereinbarung zu treffen und auf die Regelungen dieser Betriebsvereinbarung und der betreffenden Zusatzvereinbarung(en) nachweislich hinzuweisen. Dem Betriebsrat ist eine Kopie der jeweiligen Verträge zur Verfügung zu stellen.

6.5 Benutzerservice / Auskunftsperson / Helpdesk

Hard- und Software der IKT-Systeme werden durch ein Benutzerservice betreut. Es ist sicherzustellen, dass für an Bildschirmarbeitsplätzen Beschäftigte Ansprechpartner 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/r Systembetreuers/-in in eine fremde Anwendung ist durch ein optisches Signal zu kennzeichnen. Der Ausstieg des/r Systembetreuers/-in 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.

6.6 Fernwartung

Bei Fernwartung ist sicherzustellen, dass personenbezogene Daten nicht missbräuchlich verwendet werden können (z.B. über vertragliche Regelungen zur Datensicherheit). Dem Betriebsrat ist eine Kopie der jeweiligen Verträge zur Verfügung zu stellen.

Der PDSK ist über den Stand der Fernwartungseinrichtungen auf Verlangen, mindestens aber einmal jährlich, Bericht zu erstatten.

7) RECHTE des BETRIEBSRATES

7.1 Informationspflichten des Unternehmens

Das Unternehmen verpflichtet sich, dem Betriebsrat folgende Übersicht zur Verfügung zu stellen, die laufend aktualisiert wird (§§ 89 ff, 91 ArbVG):

- alle Systeme, die personenbezogene Daten verwenden, inklusive einer allgemein verständlichen Kurzbeschreibung und dem Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO.
- Personaldatenübermittlung und Auftragsdatenverarbeitung.

- Einladungen zu Veranstaltungen/Sitzungen, die in Zusammenhang mit der Einführung oder Änderung von IKT-Systemen mit personenbezogenen Datenverwendungen stehen.
- Protokolle aller Sitzungen und Veranstaltungen, die in Zusammenhang mit der Einführung oder Änderung von IKT-Systemen zur personenbezogenen Datenverwendung im Sinne der §§ 96 und 96a ArbVG stehen.

7.2 Informationsrechte des Betriebsrates

Bei allen eingesetzten IKT-Systemen sind auf Anforderung des Betriebsrates die Informationen laut Anhang 1 zur Verfügung zu stellen:

Für zukünftige (geplante) IKT-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 Projektleiter, System-Verantwortlichen und etwaiger Teilprojektleiter, sowie der involvierten Projekt-Team-Mitglieder
- Bekanntgabe eventueller externer Berater und Programmierer
- Gesamtkosten des Projektes

Sofern ein IKT-System die Verwendung von personenbezogenen Beschäftigtendaten möglich macht, ist bereits in der Planungsphase, d.h. vor Einführung bzw. Veränderung des IKT-Systems die PDSK (vgl. Pkt. 4) und der Betriebsrat einzubinden. Diese Systemänderungen oder -entwicklungen sind vor ihrer Implementierung zu dokumentieren und der PDSK zur Verfügung zu stellen.

7.3 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 (Leseberechtigung) zur Verfügung zu stellen, die ihm die Kontrolle der IKT-Systemen ermöglicht.

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 – insbesondere, wenn ein Verstoß gegen Bestimmungen dieser RBV oder einer Zusatzvereinbarung festgestellt wurde.

7.4 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 Arbeitgeber.

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

8) RECHTE der BESCHÄFTIGTEN

8.1 Information über Rechte und Pflichten

Alle Beschäftigten sind über ihre Rechte und Pflichten in Bezug auf die elektronische Datenverwendung und die dazu abgeschlossenen Betriebsvereinbarungen zu informieren.

Der Verantwortliche stellt den betroffenen Beschäftigten klare und leicht verständliche Informationen über geplante Datenverarbeitungen zur Verfügung. Über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling muss ausdrücklich informiert werden, in diesem Fall sind den Betroffenen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu übermitteln (Art 12-14 DSGVO) und die Betroffenen sind auf deren Widerspruchsrecht (Art 21-22 DSGVO) hinzuweisen.

Verwenden Beschäftigte personenbezogene Daten, haben sie vorher durch Unterschrift zu bestätigen, dass sie über ihre datenschutzrechtlichen Verpflichtungen im Sinne der betreffenden Betriebsvereinbarung(en) informiert wurden.

Die Konsequenzen eines Datenmissbrauches sollten in der PDSK genauer geregelt werden (z.B. zeitweiser Entzug der Zugriffsberechtigung oder Abmahnung) – idealer Weise *bevor* ein Anlassfall eintritt.

8.2 Schriftlicher Arbeitsauftrag bei Verdacht auf unzulässige Verwendung

Klargestellt wird: Verstößt die Weisung hinsichtlich der Zulässigkeit einer Verarbeitung oder Übermittlung gegen höherrangige Bestimmungen (insb DSGVO und Datenschutz-Anpassungsgesetz), so ist sie nichtig und muss nicht befolgt werden. Sind Beschäftigte über die Zulässigkeit einer Verarbeitung oder Übermittlung im Zweifel, sind sie berechtigt, von ihren Vorgesetzten einen schriftlichen Arbeitsauftrag einzufordern.

8.3 Auskunftsrecht

Alle Beschäftigten erhalten auf Anforderung einmal jährlich eine kurze, allgemein verständliche Auflistung im Sinne des Art 15 DSVGO.

Die Art der Auflistung (z.B. Intranet-Veröffentlichung) kann für die jeweiligen IKT-Systeme in der PDSK beschlossen werden.

8.4 Richtigstellungs- bzw. Löschungsrecht (Art 16 ff DSGVO)

Alle Beschäftigten haben das Recht, Daten richtig stellen bzw. löschen zu lassen, wenn sie nicht berechtigt ermittelt wurden, wenn sie nicht richtig sind, oder für den vorgesehenen Zweck nicht (mehr) erforderlich sind. Diesen Beschäftigten und dem zuständigen Betriebsrat ist eine Überprüfungsmöglichkeit über die Korrektur bzw. Löschung einzuräumen. Entsteht Uneinigkeit über die Richtigkeit von Daten und kann das Unternehmen die Richtigkeit nicht nachweisen, so sind diese Daten zu löschen. Bis zur Klärung eines allfällig vorliegenden Sachverhalts hat die betroffene Person das Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO).

8.5 Umgang mit privaten Dokumenten und E-Mails

Die Nutzung der betrieblichen IKT-Systeme für private Zwecke ist in angemessenem Ausmaß zulässig. Es können alle Beschäftigten, auf ihren Arbeitsspeichern 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. Download aus dem Internet, Installieren neuer Software).

9) BESTEHENDE und NEUE SYSTEME

In den Zusatzvereinbarungen sind je IKT-System zumindest folgende Informationen zu vereinbaren

- Verwendungszweck(e)
- Systemteile, Module
- verwendete Datenarten inklusive Kategorisierung
- Auswertungen
- Berechtigungskonzept
- Schnittstellen, Empfängerkreise und mögliche Dienstleister
- Löschfristen

10) INKRAFTTRETEN und VERTRAGSDAUER

Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft und gilt unbefristet.

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

Zeichnungsbevollmächtigte

für das Unternehmen

.....

für den Betriebsrat

.....

ANHANG 1: Information zu IKT-System

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

1. Name des IKT-Systems (Datenanwendung), Versionsbezeichnung und Anbieter
2. die jeweiligen Systembeschreibungen / Benutzerhandbücher
3. betriebliche(r) Verantwortliche(r) / Ansprechperson(en)
4. Dokumentation aus dem Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO
5. Mandanten, die personenbezogene Echtdaten verwenden (z.B. Testsystem, Konsolidierungssystem, Produktivsystem)
6. eingesetzte Systemteile / Module
7. Verwendungszweck der Datenanwendung
8. Ort der Datenhaltung/-verwaltung (bei Dienstleister, nähere Angaben zum Dienstleister)
9. betroffene Personengruppe
10. Standort und Art der Datenerfassungsgeräte (z.B. Terminals, Kameras, Automaten, …)
11. die verwendeten Datenarten und Datenkategorien
12. ein Verzeichnis personenbezogener Auswertungen mit Beispielen
13. Schnittstellen (Import und Export) zu anderen IKT-Systemen
14. Zugriffsberechtigungsverzeichnis und mögliche Empfängerkreise
15. Löschfristen
16. Technische und organisatorische Maßnahmen gemäß Art 32 Abs 1 DSGVO
17. Die Ergebnisse der allfällig durchgeführten Datenschutzfolgenabschätzung sowie der Konsultation der Datenschutzbehörde (gem Art 35 f DSGVO)
18. Auflistung der allfällig getroffenen Maßnahmen im Zusammenhang mit Datenschutz durch Technik und allfällig eingeführte datenschutzfreundliche Voreinstellungen
19. Auflistung allfällig eingeführter Verfahrensregeln und Zertifizierungen
20. Name des/der allfällig bestellten betrieblichen Datenschutzbeauftragten (gem 37 ff DSGVO)
21. Allfällig vorhandener Tätigkeitsbericht des betr. DSB
22. Form der Protokollierung

ANHANG 2: Datenkategorisierung

Zwecke der Kategorisierung sind

- Aufbereitung der personenbezogenen Daten für die interne Dokumentation der Datenanwendungen (Art 30 DSGVO) und für eine allfällige Datenschutzfolgeabschätzung (Art 35 DSGVO)
- Grundlage für organisatorische und technische Regelungen bei der Datenverwendung
- Sensibilisierung der Führungskräfte und der Beschäftigten für Datenschutz und Datensicherheit

Die personenbezogenen Beschäftigtendaten werden für jedes eingesetzte IKT-System nach den folgenden vier Kategorien unterteilt.

Da idente Datenfelder in verschiedenen IKT-Systemen unterschiedliche Bedeutung besitzen können, hat diese Unterteilung für jedes IKT-System, für das eine Zusatzvereinbarung abgeschlossen wird, zu erfolgen. Der Vorschlag, welches Datenfeld in welche Kategorie fällt, kann in der innerbetrieblichen Personaldatenschutzkommission (vgl. Pkt.4) erfolgen

Folgende vier Kategorien werden eingeführt:

Kategorie A: Allgemeine Daten zur Person.

Diese Daten umfassen die geschäftlichen Kommunikationsdaten (z.B.: Name, Organisationseinheit, Firmenanschrift, Büroraum, Telefonnummer, E-Mail-Adresse). Diese Daten können in einem Unternehmensadressbuch gefunden werden. Sie stehen zwar mit den einzelnen Beschäftigten in Verbindung, gehören aber zu den Arbeitsmitteln im Unternehmen.

Kategorie B: Daten zur Person die verpflichtend aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag für einen eindeutigen Zweck verwendet werden müssen.

Diese Daten müssen vom Unternehmen verwendet werden. In diesen Fällen werden die Daten benötigt, um gesetzlichen Forderungen bzw. vertraglichen Verpflichtungen (eindeutiger und rechtmäßiger Zweck im Sinne von Art 5 Abs 1 lit a und b DSGVO) nachkommen zu können. Darüber hinaus können in dieser Kategorie weitere Datenarten in Abstimmung zwischen Arbeitgeber – Betriebsrat angeführt werden. (z.B.: Anschrift, Arbeitszeit, Urlaubsanspruch, Bankverbindung, Qualifikationen, betriebliche Funktion.)

Kategorie C: Schutzwürdige Daten der Beschäftigten sowie Daten, für die keine gesetzliche Verpflichtung zur Verwendung besteht.

Diese Daten gehören zum Teil zu den Stammdaten (werden daher auch für einzelne Verarbeitungen wie z.B. zur Entgeltberechnung benötigt), sind aber primär dem Privatbereich der Beschäftigten zuzuordnen und stehen nicht direkt mit dem Unternehmen in Verbindung (z.B.: Familienstand, Zweitwohnsitz). Hierunter fallen auch Daten, die aus Sicht der betroffenen Beschäftigten einem erhöhten Schutzinteresse unterliegen (z.B.: Pfändungen, betriebliche Darlehen).

Weiters fallen in diese Kategorie Daten, die Aussagen über das Verhalten einzelner Beschäftigter enthalten können (z.B.: Fehlzeiten und Mehrarbeit, Leistungsstunden für diverse Aufträge/Projekte die Vergleiche zulassen, leistungsabhängige Entgeltbestandteile, Beurteilungen, vereinbarte Ziele aus Mitarbeitergesprächen, ...)

Kategorie D: Sensible Daten. Besondere Kategorien personenbezogener Daten und Daten mit erhöhten Schutzanforderungen im Sinn des Art 9 und 10 DSGVO

Darunter fallen Daten der Beschäftigten über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben, sowie biometrische (z.B. Irisscan, Fingerprint) und genetische Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten.

ACHTUNG: Nach Vorstrafen und laufenden Ermittlungsverfahren darf der Arbeitgeber idR gar nicht fragen, geschweige denn darf er solche Daten speichern. Ausnahme: Wenn zwischen dem Tätigkeitsbereich des Arbeitnehmers und einem begangenen Delikt ein Zusammenhang besteht (z.B. KassierIn in einem Geldinstitut und Vermögensdelikte; LehrerInnen und Kindesmissbrauchsdelikte).

ANHANG 3: Geschäftsordnung

Zur Bewältigung der organisatorischen Abläufe hat die PDSK (nach ihrer Konstituierung) eine Geschäftsordnung mit folgendem Mindestinhalt festzulegen, die dieser Betriebsvereinbarung angehängt wird, ohne allerdings Bestandteil zu sein:

- Vorsitzführung
- Protokollführung
- Art der Beschlussfassung
- Art der Einberufung
- Tagungsintervall

Mögliche Inhalte der Geschäftsordnung:

- Die Konstituierung hat innerhalb drei Monaten nach Abschluss dieser Betriebsvereinbarung durch Wahl eines/-r Vorsitzenden zu erfolgen.
- Die PDSK ist beschlussfähig, wenn sowohl von Seite der Unternehmensleitung, als auch von Seite des Betriebsrats zwei Mitglieder anwesend sind. Gültige Beschlüsse können nur einstimmig gefasst werden und sind zu protokollieren.
- Die PDSK tagt vierteljährlich.
- Der/die Vorsitzende hat auch auf Verlangen eines Kommissionsmitgliedes, unter Angabe des Grundes, binnen fünf Arbeitstagen eine Sitzung einzuberufen. Jede Einberufung hat eine schriftliche Tagesordnung zu enthalten und ist spätestens zwei Arbeitstage vor der Sitzung allen Kommissionsmitgliedern zu übergeben.
- Zwischenzeitliche Einberufungen durch den/die Vorsitzende/n sind möglich.