Martina Chlestil, Adriana Mandl, Thomas Riesenecker-Caba

Verarbeitung von personenbezogenen Mitarbeiter:innen-Daten

Mitbestimmung und Datenschutz

5 Praktische Gewerkschaftsarbeit

Praktische Gewerkschaftsarbeit 5

Verarbeitung von personenbezogenen Mitarbeiter:innendaten

Mitbestimmung und Datenschutz

Martina Chlestil, Adriana Mandl,
Thomas Riesenecker-Caba

Verarbeitung von personenbezogenen Mitarbeiter:innendaten

Mitbestimmung und Datenschutz

Dieses Skriptum ist für die Verwendung im Rahmen der Bildungsarbeit des Österreichischen Gewerkschaftsbundes, der Gewerkschaften und der Kammern für Arbeiter und Angestellte bestimmt.

Zeichenerklärung

 Hinweise

 Beispiele

 Zitate

Rechtsstand: August 2025

Stand: August 2025

Impressum:
Umschlaggestaltung: Thomas Jarmer
Medieninhaber: Verlag des ÖGB GmbH, Wien

Herstellung: Verlag des ÖGB GmbH, Wien
Verlags- und Herstellungsort: Wien
Druck: CITYPRESS GesmbH, Neutorgasse 9, 1010 Wien
Printed in Austria

Inhalt

Inhalt

SKRIPTEN ÜBERSICHT

VÖGB

SOZIALRECHT

SR-1	Grundbegriffe des Sozialrechts
SR-2	Sozialpolitik im internationalen Vergleich
SR-3	Sozialversicherung – Beitragsrecht
SR-4	Pensionsversicherung I: Allgemeiner Teil
SR-5	Pensionsversicherung II: Leistungsrecht
SR-6	Pensionsversicherung III: Pensionshöhe
SR-7	Krankenversicherung I: Allgemeiner Teil
SR-8	Krankenversicherung II: Leistungsrecht
SR-9	Unfallversicherung
SR-10	Arbeitslosenversicherung I: Allgemeiner Teil
SR-11	Arbeitslosenversicherung II: Leistungsrecht
SR-12	Insolvenz-Entgeltsicherung
SR-13	Finanzierung des Sozialstaates
SR-14	Pflege und Betreuung

Die einzelnen Skripten werden laufend aktualisiert.

ARBEITSRECHT

AR-1	Kollektive Rechtsgestaltung
AR-2A	Betriebliche Interessenvertretung
AR-2B	Mitbestimmungsrechte des Betriebsrates
AR-2C	Rechtstellung des Betriebsrates
AR-3	Arbeitsvertrag
AR-4	Arbeitszeit
AR-5	Urlaubsrecht
AR-6	Entgeltfortzahlung im Krankheitsfall
AR-7	Gleichbehandlung im Arbeitsrecht
AR-8A	ArbeitnehmerInnenschutz I: Überbetrieblicher ArbeitnehmerInnenschutz
AR-8B	ArbeitnehmerInnenschutz II: Innerbetrieblicher ArbeitnehmerInnenschutz
AR-9	Beendigung des Arbeitsverhältnisses
AR-10	Arbeitskräfteüberlassung
AR-11	Betriebsvereinbarung
AR-12	Lohn(Gehalts)exekution
AR-13	Berufsausbildung
AR-14	Wichtiges aus dem Angestelltenrecht
AR-15	Betriebspensionsrecht I
AR-16	Betriebspensionsrecht II
AR-18	Abfertigung neu
AR-19	Betriebsrat – Personalvertretung Rechte und Pflichten
AR-21	Atypische Beschäftigung
AR-22	Die Behindertenvertrauenspersonen

GEWERKSCHAFTSKUNDE

GK-1	Was sind Gewerkschaften? Struktur und Aufbau der österreichischen Gewerkschaftsbewegung
GK-2	Geschichte der österreichischen Gewerkschaftsbewegung von den Anfängen bis 1945
GK-3	Die Geschichte der österreichischen Gewerkschaftsbewegung von 1945 bis heute
GK-4	Statuten und Geschäftsordnung des ÖGB
GK-5	Vom 1. bis zum 19. Bundeskongress
GK-7	Die Kammern für Arbeiter und Angestellte
GK-8	Die sozialpolitischen Errungenschaften des ÖGB
GK-9	Geschichte der Kollektivverträge

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen:
www.voegb.at/skripten

1 Einleitung

Die letzten Jahrzehnte waren von umfangreichen technologischen Umbrüchen in der betrieblichen IT-Landschaft (aber nicht nur dort) geprägt.

Die Verbreitung des Internets, verbunden mit der Möglichkeit einer weltweiten Vernetzung, eine allgegenwärtige Nutzung mobiler Geräte wie z. B. Smartphones und nicht zuletzt die Verlagerung der eigentlichen Datenverarbeitung in die Cloud sind Zeichen dieses nachhaltigen betrieblichen Wandels. In den letzten Jahren wurde zusätzlich das Thema „Künstliche Intelligenz" (KI) durch die massive Nutzung von Sprachmodellen (Large Language Models) wie ChatGPT oder Copilot nach Jahrzehnten wiederbelebt.

Neben den technischen Entwicklungen vergrößerte sich jedoch auch die Gefahr von Angriffen auf die betriebliche IT über Netzwerke oder Geräte. Schadsoftware, Viren oder höchst professionelle Cyberangriffe erfordern umfassende Maßnahmen zum Datenschutz und zur Systemsicherheit.

In diesem Umfeld versuchen betriebliche Interessenvertretungen wie Betriebsrat oder Personalvertretung, die Verarbeitung von personenbezogenen Daten der Mitarbeiter:innen auf datenschutz- und arbeitsrechtlich konforme Weise erfolgen zu lassen und die im Arbeitsverfassungsgesetz geforderte Mitbestimmung und den Abschluss von Betriebsvereinbarungen umzusetzen.

Zahlen einer österreichweiten Betriebsratsbefragung[1] zeigen, dass dies in vielen Fällen Betriebsrat und Personalvertretung vor große Herausforderungen stellt.

Diese Schriftenreihe gibt hier Unterstützung, indem

» Wissen über die Verarbeitung personenbezogener Mitarbeiter:innendaten vermittelt,

» zentrale Fragen zu Mitbestimmung und Datenschutz anschaulich erklärt, und

» Hinweise zur betrieblichen Herangehensweise geliefert

werden.

SKRIPTEN ÜBERSICHT

VÖGB

WIRTSCHAFT

WI-1 Einführung in die Volkswirtschaftslehre und Wirtschaftswissenschaften

WI-2 Konjunktur

WI-3 Wachstum

WI-4 Einführung in die Betriebswirtschaftslehre

WI-5 Beschäftigung und Arbeitsmarkt

WI-6 Lohnpolitik und Einkommensverteilung

WI-9 Investition

WI-10 Internationaler Handel und Handelspolitik

WI-12 Steuerpolitik

WI-13 Bilanzanalyse

WI-14 Der Jahresabschluss

WI-16 Standort-, Technologie- und Industriepolitik

Die einzelnen Skripten werden laufend aktualisiert.

POLITIK UND ZEITGESCHICHTE

PZG-1A Sozialdemokratie und andere politische Strömungen der ArbeiterInnenbewegung bis 1945

PZG-1B Sozialdemokratie seit 1945

PZG-2 Christliche Soziallehre

PZG-4 Liberalismus/Neoliberalismus

PZG-6 Rechtsextremismus

PZG-7 Faschismus

PZG-8 Staat und Verfassung

PZG-9 Finanzmärkte

PZG-10 Politik, Ökonomie, Recht und Gewerkschaften

PZG-11 Gesellschaft, Staat und Verfassung im neuzeitlichen Europa, insbesondere am Beispiel Englands

PZG-12 Wege in den großen Krieg

PZG-14 Die Geschichte der Mitbestimmung in Österreich

SOZIALE KOMPETENZ

SK-1 Grundlagen der Kommunikation

SK-2 Frei reden

SK-3 NLP

SK-4 Konfliktmanagement

SK-5 Moderation

SK-6 Grundlagen der Beratung

SK-7 Teamarbeit

SK-8 Führen im Betriebsrat

SK-9 Verhandeln

SK-10 Politische Rhetorik

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen: www.voegb.at/skripten

2 Stand der Technik

Die Verarbeitung personenbezogener Mitarbeiter:innendaten erfolgt in den Betrieben zu unterschiedlichen Zwecken, von der Unterstützung der Bewältigung betrieblicher Aufgaben und Optimierung der betrieblichen Abläufe bis hin zur Kontrolle von Beschäftigten. Die Vielfalt der technischen Systeme, die im Bereich der Informationsverarbeitung und Kommunikation zum Einsatz kommen, ist nur noch schwer zu überblicken, und die gesetzlich notwendige Einbeziehung des Betriebsrats, insbesondere nach den Bestimmungen der §§ 96, 96a und 97 ArbVG, hängt oft von der aktiven Information der Arbeitgeberin bzw. des Arbeitgebers und den zur Verfügung gestellten Informationen ab. Auch abseits der Regelung von konkreten IT-Systemen erfolgt die Automatisierung in unterschiedlichsten Bereichen, und Betriebsräte sind gemäß § 109 ArbVG unter anderem bei Änderungen der Arbeits- und Betriebsorganisation und der Einführung von Rationalisierungs- und Automatisierungsmaßnahmen von erheblicher Bedeutung von der bzw. dem Arbeitgeber:in verpflichtend zu informieren.

Denn erst nach umfassender Information und Analyse der technischen Beschreibungen ist es für Betriebsräte nachvollziehbar,

- welche technischen und organisatorischen Veränderungen die Einführung eines IT-Systems bewirkt,
- welche Daten der Beschäftigten verarbeitet werden,
- welche Auswertungen oder Analysen das betreffende System ermöglicht,
- ob andere Systeme mit personenbezogenen Daten beliefert werden,
- wer eigentlich Zugriff auf die personenbezogenen Daten und Systemfunktionen besitzt und
- wie die Verarbeitung der Daten kontrolliert werden kann (z. B. über Protokolle).

2.1 Personenbezogene Daten

Wenden wir uns zuerst der Frage zu, was eigentlich unter personenbezogenen Daten verstanden wird und welche Kategorien von personenbezogenen Daten unterschieden werden können.

Personenbezogene Daten 2.1

Die **Datenschutz-Grundverordnung** (DSGVO) definiert personenbezogene Daten in ihrem Art 4 Z 1 DSGVO wie folgt:

Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ([...] „betroffene Person") beziehen.

Als „identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen (die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind), identifiziert werden kann."

Eindeutig identifiziert werden kann eine Person aufgrund ihres Namens. Hier ist es für die Betroffenen leicht nachzuvollziehen, dass aufgrund dieser Information ihre Identität erkennbar ist. Diese Datenarten werden oft als Teil der Stammdaten (ein Begriff aus der Informatik) beschrieben. Stammdaten sind allgemeine Angaben zu einer bestimmten Person und ändern sich im Laufe des Berufslebens wenig bis gar nicht (z. B. Sozialversicherungsnummer, Privatadresse, Kostenstelle, Bankverbindung).

Etwas schwieriger ist die Wahrnehmung der Daten, über die eine Person identifizierbar ist. Tagtäglich wird eine Vielzahl an Daten über einzelne Beschäftigte gespeichert, die diese durch ihre Tätigkeit und die Verwendung von technischen Systemen erzeugen (z. B. Abholen eines Kopierauftrags, Versenden einer E-Mail, Arbeit an einer Produktionsmaschine, Fahrt mit einem Firmenfahrzeug). Wann immer die Möglichkeit besteht, durch Verknüpfung unterschiedlicher Informationen auf eine Person zu schließen, ist diese (im Sinne der Begriffsdefinition der DSGVO) identifizierbar.

Beispiele:

» *Eine Person meldet sich über ihre personifizierte Chip(karte) oder ein nur ihr bekanntes Kennwort an einer Kopier-/Druckstation an, um einen Druckauftrag zu erhalten.*

2 Stand der Technik

» *Ein:e Arbeiter:in in einem Produktionsbetrieb meldet sich zu Schichtbeginn über Terminal an einer Maschine an und über den Schicht-/Dienstplan ist nachvollziehbar, wer diese Person ist.*

» *Ein:e Fahrer:in ist mit einem Firmenfahrzeug unterwegs, das ihr bzw. ihm zuvor zugeteilt wurde oder das sie bzw. er über den Fahrzeugpool reserviert hat.*

So können für das zweite angeführte Beispiel die erzeugten Stückzahlen an der Produktionsmaschine oder deren Stillstandzeiten einer Person zugeordnet werden (diese ist identifizierbar), und somit sind die Daten personenbezogen.

Auch der Standort des Fahrzeuges aus unserem dritten Beispiel oder Fahrzeugdaten (aus der On-Board-Diagnose), wie Benzinverbrauch oder Geschwindigkeit, ermöglichen Rückschlüsse auf das Fahrverhalten und den konkreten zurückgelegten Weg inkl. möglicher Pausen, und diese Daten sind somit personenbezogen.

In diesem Zusammenhang spricht man von Bewegungsdaten. Diese Daten fallen durch das Arbeiten im Unternehmen bzw. die Nutzung betriebseigener Arbeitsmittel, wie PC, Smartphone, Produktionsmaschinen oder Firmenfahrzeug, an.

Erwägungsgrund (in Folge ErwG) 26[2]der DSGVO liefert hier einen weiteren wichtigen Hinweis: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren."

Daher spricht die DSGVO von personenbezogenen Daten, wenn eine Zuordnung zu einer natürlichen Person möglich ist, und zwar über

» eine Kennnummer (z. B. Maschinenbezeichnung, zugewiesener Arbeitsplatz im Callcenter),

» Standortdaten (z. B. GPS-Daten eines Fahrzeugs oder eines mobilen Endgeräts wie Smartphone oder Tablet, bei denen die GPS-Funktion eingeschaltet ist),

» eine Online-Kennung (z. B. IP-Adresse eines PCs, wobei die IP-Adresse für jedes Endgerät, das sich in einem Netzwerk anmeldet, eindeutig ist, sonst könnten

abgerufene Informationen nicht zum richtigen Arbeitsplatz transportiert werden, ähnlich der Postadresse, die zur Übermittlung von Briefen notwendig ist), oder

» ein oder mehrere besondere(s) Merkmal(e) (z. B. Verknüpfung diverser Informationen im Rahmen einer Onlinebefragung).

Wann immer personenbezogene Mitarbeiter:innendaten verarbeitet werden, sind die Bestimmungen des Datenschutzrechts und der Arbeitsverfassung einzuhalten.

2.2 Überblick der personenbezogenen Daten

Einer der zentralen Grundsätze des Datenschutzrechts der bei der Verarbeitung von Daten zu berücksichtigen ist, ist die sogenannte Zweckbestimmung, d. h., es ist ein Zweck anzugeben, warum eine personenbezogene Datenverarbeitung notwendig erscheint.

Diese Zwecke können sehr unterschiedlicher Natur sein, beginnend bei der Vergabe von Berechtigungen (User-ID), um in einem System arbeiten zu können, über die Erfassung gehaltsrelevanter Daten (z. B. Zeiterfassung, Bankverbindung), die Dokumentation der täglichen Arbeit (z. B. bearbeitete Belege) bis hin zur Gewährleistung der Sicherheit im Unternehmen (z. B. Zutrittskontrolle, Videokontrolle).

Um hier nicht den Überblick zu verlieren, empfiehlt es sich, die im Unternehmen verarbeiteten personenbezogenen Daten nach verschiedenen Anwendungsbereichen zu unterscheiden. Diese Systematik (z. B. Einführung einer Datenklassifizierung) könnte auch in einer Rahmen-Betriebsvereinbarung (mehr dazu in Kapitel 6) Verwendung finden.

Eine Klassifizierung ist beim Umgang mit Betriebs- und Geschäftsgeheimnissen in Betrieben nicht ungewöhnlich.

So klassifiziert das IT-Sicherheitshandbuch des Bundes[3] verschiedene Stufen der Vertraulichkeit von Informationen und empfiehlt darauf abgeleitet, Regeln für den betrieblichen Umgang (oft als Policies bezeichnet) festzuschreiben (z. B.

wem darf welche Art von Information offengelegt werden oder welche Daten dürfen per E-Mail versendet werden).

Diese **Vertraulichkeitsstufen** („Labels") werden oft wie folgt beschrieben:

- öffentlich (z. B. Angaben, die über eine Unternehmenswebseite abrufbar sind wie Adresse, Namen der Geschäftsführer:innen),
- intern (z. B. internes Mitarbeiter:innenverzeichnis),
- vertraulich (z. B. Lohn- bzw. Gehaltsdaten, Verträge mit Kundinnen und Kunden, Finanzdaten),
- streng vertraulich (z. B. Dokumente der Betriebsärztin bzw. des Betriebsarztes, Vorstandsprotokolle).

Abgeleitet von diesem Ansatz können personenbezogene Mitarbeiter:innendaten im Sinne der Bestimmungen der DSGVO bzw. des DSG und des ArbVG nach den folgenden Datenschutzklassen unterteilt werden.

Klasse	Beschreibung	Erklärung/Beispiele
A	Funktionsdaten	Sind zur Berechtigungssteuerung in den IT-Systemen notwendig Beispiele: Name, ID, Berechtigungsrolle
B	Stammdaten	Diese Daten umfassen die Stamm- und Kommunikationsdaten und die organisatorische Zuordnung somit allgemeine Angaben zur Person. Beispiele: Name, Organisationseinheit, Firmenanschrift, Büroraum, Telefonnummer, E-Mail-Adresse
C	Abwicklungsdaten	Diese Daten müssen zur Erfüllung einer rechtlichen Verpflichtung aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag für einen eindeutigen und berechtigten Zweck verarbeitet werden. Beispiele: Entgeltberechnung, Zeitbuchungen

Überblick der personenbezogenen Daten

Klasse	Beschreibung	Erklärung/Beispiele
D	Geschäftsdaten	Diese Daten werden durch die Arbeit mit IT-Systemen erfasst und dokumentieren Tätigkeiten der Arbeitnehmer:innen. Beispiele: Bearbeitungsdauer (Beginn – Ende) eines Auftrages, Anzahl der täglichen Kontierungen
E	besonders schutzwürdige (sensible) und strafrechtlich relevante Daten	Diese Daten werden nach Art 9 und 10 DSGVO als besonders schutzwürdig eingestuft und dürfen nur für eindeutigen und berechtigten Zweck verarbeitet werden.
F	Geo-/Lokationsdaten	Diese Daten erlauben Rückschlüsse auf den Standort einer Person bzw. eines dieser Person überantworteten Arbeitsmittel (Laptop, Smartphone, Fahrzeug)
G	Audio- und Bilddaten	Audio- oder Bilddaten (z. B. Video), die eindeutig einer Person zugewiesen werden können. Beispiele: Aufzeichnung Videomeeting, Bilder einer Überwachungskamera
H	Protokolldaten	Das Arbeiten in einem IT-System wird je IT-System in unterschiedlicher Detaillierung protokolliert. Andere Bezeichnungen für Protokolldaten sind diagnostische Daten, Verkehrs- oder Telemetriedaten. Beispiele: Zeitpunkt des Logins und das dabei verwendete Gerät, Absenden eines Druckauftrages, Öffnen einer E-Mail, Änderung oder Löschen einer Information

Klasse	Beschreibung	Erklärung/Beispiele
I	Inhaltsdaten	Daten/Informationen/Dokumente, die durch das individuelle Arbeiten der Arbeitnehmer:innen in den unterschiedlichen Services/Komponenten entstehen und personenbezogene Informationen enthalten können. Beispiele: Inhalt einer E-Mail oder eines Chats

2.3 Was sind pseudonymisierte Daten?

Die DSGVO führt als eine Datenschutzmaßnahme die Pseudonymisierung von personenbezogenen Daten an. Definiert wird dieser Begriff in Art 4 Z 5 DSGVO als

> **„die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".**

Das bedeutet, dass statt einer eindeutigen Zuordnung einer bestimmten Person (z. B. über deren Personalnummer) dieses Datum pseudonymisiert wird, d. h. durch einen nur der durchführenden Person (bzw. einem äußerst kleinen Kreis) bekannten Code (z. B. ABC#456) ersetzt wird. Anhand dieses Codes wäre dann eine Person nicht direkt erkennbar (identifizierbar). Die Verbindung zwischen der eindeutigen Information (in unserem Beispiel der Personalnummer) und dem stattdessen verwendeten Code wäre in einer gesicherten (z. B. verschlüsselten) Tabelle zu hinterlegen.

Was sind pseudonymisierte Daten? 2.3

Pseudonymisierte Daten sind jedoch keine anonymisierten Daten, sondern es wird nur die Identifizierbarkeit einer Person erschwert. Das führt auch ErwG 26 der DSGVO aus:

„Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden."

3 Technische Systeme

In den letzten Jahrzehnten haben sich die Anwendungsbereiche, in denen technische Systeme zu Einsatz kommen, großflächig erweitert. Kaum ein betrieblicher Bereich kommt mehr ohne Datenverarbeitung und die Anwendung technischer Systeme, Maschinen oder Geräte aus.

Dies führt auch dazu, dass immer mehr personenbezogene Mitarbeiter:innendaten für unterschiedliche Zwecke verarbeitet werden.

In der Vergangenheit waren es vor allem Anwendungsgebiete wie Personalverrechnung, Zeiterfassung, Zutritts- oder Videokontrolle bzw. branchenspezifische Anwendungsbereich wie Callcenter-Steuerung oder Produktionsplanung. Durch die Vernetzung von Geräten (z. B. Smartphones) und den globalen Datenaustausch zwischen Betrieben (z. B. Internet, Cloud-Computing) sind nicht nur die Anwendungsbereiche deutlich vermehrt worden, sondern es müssen auch im Bereich der Systemsicherheit zur Abwehr von Cyberangriffen unterschiedlichste technische Systeme eingesetzt werden.

Hier den Überblick zu bewahren, ist für den Betriebsrat nicht immer leicht.

Die folgende Abbildung gibt einen Überblick über die verschiedenen Einsatzgebiete[4] und mögliche (datenschutzrechtliche) Verwendungszwecke. Inwieweit diese IT-Systeme im jeweils eigenen Unternehmen zum Einsatz kommen, ist einerseits von der bzw. dem Arbeitgeber:in dem Betriebsrat nach § 91 ArbVG mitzuteilen, zum andern sind personenbezogene Datenverarbeitungen in einem Verzeichnis (geregelt durch Art 30 DSGVO) festzuhalten.

Einsatzgebiete	Verwendungszwecke
Personalverwaltung	Personalverrechnung, Zeitwirtschaft, digitaler Personalakt, HR Cloud (SAP SuccessFactors, Workday) mit Prozessunterstützung: Personalentwicklung (Mitarbeiter:innengespräche, Skills, internes Recruiting), E-Learning (Gamification)
Kommunikations- und Kollaborationssysteme	Telefon (VoIP), MS Teams, Zoom, Viva Engage, Internet, Intranet, mobile Arbeit und Kommunikation (inkl. Apps), E-Mail

Einsatzgebiete	Verwendungszwecke
Verwaltungssoftware	Multifunktions-Chip, MDM (Mobile Device Management), Multifunktionsgeräte, Helpdesk, Benutzer:innenverwaltung (AD = Active Directory), Geräteverwaltung (IT-Asset-Management)
Kontrollsysteme	Zutritt, Video
IT-Sicherheit	Firewall, SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), ISMS (Information Security Management System), Security Training (Phishing)
Büroautomation	Microsoft 365 (Office 365 inkl. EMS = Enterprise Mobility + Security, Windows Enterprise, Dynamics 365)
ERP-Systeme (außer HCM/HR)	Enterprise-Resource-Planning (Finanzwesen, Lagerverwaltung, Einkauf, Vertrieb, CRM, ...)
Branchenspezifische Lösungen	Produktion (MES: MDE, BDE, ...), Callcenter, Außendienst (Flottenmanagement, GPS), M2M (machine to machine), Borddaten (in Pkw, Lkw, Stapler - Crash Sensoren), Tätigkeitserfassung, Qualitätssicherung (Mystery Calls), Ausgabeautomaten
Online-Befragungstools	Mitarbeiter:innenumfragen, Stimmungsbarometer
Künstliche Intelligenz (KI/AI), Big Data	Data Lake, Business Intelligence/Data Warehouse, Künstliche Intelligenz (maschinelles Lernen, Logik- und wissensgestützte Konzepte, statistische Ansätze, LLM, general purpose AI)
Compliance and Governance	Hinweisgeber:innensystem (Whistleblowing), HSE oder EHS (Health-Safety-Environment), Systeme zur Entgelttransparenz

3 Technische Systeme

Einsatzgebiete	Verwendungszwecke
Mitarbeiter:innen in anderer Rolle	als Kundin oder Kunde im betriebsinternen CRM-System oder in der Kund:innenverwaltung/Klient:innenverwaltung, vor Eintritt in das Unternehmen als Bewerber:in (Recruiting, Onboarding)

Um die im eigenen Betrieb eingesetzten IT-Systeme beurteilen zu können, sind, wie oben bereits angeführt, umfangreiche Informationen notwendig, um in Folge – und in Kooperation mit Gewerkschaft und Arbeiterkammer – die technischen IT-Systeme gemäß den Bestimmungen der Arbeitsverfassung durch Betriebsvereinbarung regeln zu können.

In den nächsten Kapiteln werden zum einen die dazu notwendigen arbeits- und datenschutzrechtlichen Bestimmungen erklärt und zum anderen mittels Checkliste und „Spielregeln" gezeigt, wie auf diese vielfältige personenbezogene Datenverarbeitung reagiert werden kann.

VÖGB/AK-SKRIPTEN

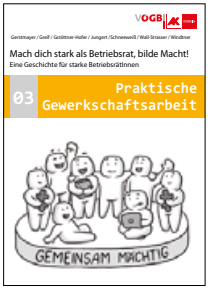
Die Skripten sind eine Alternative und Ergänzung zum VÖGB/AK-Bildungsangebot und werden von ExpertInnen verfasst, didaktisch aufbereitet und laufend aktualisiert.

UNSERE SKRIPTEN UMFASSEN FOLGENDE THEMEN:

- Arbeitsrecht
- Sozialrecht
- Gewerkschaftskunde
- Praktische Gewerkschaftsarbeit
- Internationale Gewerkschaftsbewegung
- Wirtschaft
- Wirtschaft – Recht – Mitbestimmung
- Politik und Zeitgeschehen
- Soziale Kompetenz
- Humanisierung – Technologie – Umwelt
- Öffentlichkeitsarbeit

SIE SIND GEEIGNET FÜR:

- Seminare
- ReferentInnen
- Alle, die an gewerkschaftlichen Themen interessiert sind.

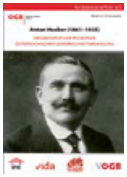


Nähere Infos und kostenlose Bestellung:
www.voegb.at/skripten
E-Mail: skripten@oegb.at
Adresse:
Johann-Böhm-Platz 1,
1020 Wien
Tel.: 01/534 44-39244

Die Skripten gibt es hier zum Download:

www.voegb.at/skripten

Leseempfehlung:
Reihe Zeitgeschichte und Politik



4 Arbeitsverfassung

Wie bereits oben angeführt, kommen in den Betrieben zahlreiche Informations- und Kommunikationssysteme zur Anwendung, die Beschäftigtendaten verarbeiten. Das Arbeitsverfassungsgesetz (ArbVG) stellt dem Betriebsrat Regelungen zur Verfügung, die es ihm ermöglichen, die Interessen der Arbeitnehmer:innen bei der Verarbeitung ihrer Daten im Betrieb zu wahren.

4.1 Wie ist das Verhältnis von Arbeitsverfassungsrecht und Datenschutzrecht?

Der OGH hat bereits im Jahr 2014 bestätigt, dass es sich bei den Befugnissen des Betriebsrates um Pflichtbefugnisse handelt, die durch das (damals anzuwendende) Datenschutzgesetz 2000 nicht beschränkt werden. **Seit 25. Mai 2018** gilt ein **neues Datenschutzrecht:** Das ist zum einen die Europäische Datenschutz-Grundverordnung (DSGVO) und zum anderen das Datenschutzgesetz (DSG). Zur Frage des Verhältnisses von Arbeitsverfassungsrecht und Datenschutzrecht ist festzuhalten, dass auch das „neue" Datenschutzrecht – wie schon in gleicher Weise das DSG 2000 und das DSG 1978 – generell nicht in die Betriebsverfassung eingreifen will.

Die Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG werden durch die DSGVO und das DSG nicht beschnitten. Zu beachten ist aber, dass die Datenverarbeitung durch den Betriebsrat und dessen Mitglieder ebenfalls datenschutzkonform, insbesondere unter Einhaltung entsprechender Datensicherheitsmaßnahmen etc. zu erfolgen hat.

Die Mitwirkungsbefugnisse des Betriebsrates bilden so neben dem individuellen Schutz der Arbeitnehmerin bzw. des Arbeitnehmers durch die DSGVO und das DSG eine zusätzliche Beschränkung der Arbeitgeberin bzw. des Arbeitgebers im Umgang mit Beschäftigtendaten durch kollektive Befugnisse.

Siehe dazu OGH 6 ObA 2/23x, OGH 6 ObA 1/14m sowie ausführlich *Goricnik*, FAQ Datenschutz im BR-Büro, in *Haslinger/Krisch/Riesenecker-Caba*, Beschäftigtendatenschutz (2019) 256 sowie *Auer-Mayer* in *Gahleitner/Mosler*, Arbeitsverfassungsrecht 3, 6. Auflage (2020), § 91 Rz 15.

4.2 Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG

Nachfolgend sollen die für die Betriebsratsarbeit relevanten Bestimmungen des ArbVG bei der Verarbeitung personenbezogener Beschäftigtendaten dargestellt werden.

4.2.1 Überwachungsbefugnisse

Durch die in **§ 89 Satz 1 ArbVG** enthaltene Generalklausel ist ein umfassendes Überwachungsrecht des Betriebsrates bezüglich der Einhaltung aller die Arbeitnehmer:innen berührenden Normen (z. B. arbeits-, steuer- oder sozialversicherungsrechtlichen Inhalts) sichergestellt. Dabei kommt es nicht darauf an, ob sich solche Normen aus Gesetz, Verordnung, Kollektivvertrag, Satzung, Mindestlohntarif oder Betriebsvereinbarung, Bescheid oder Einzelarbeitsvertrag oder etwa aus schuldrechtlichen Vereinbarungen zwischen Betriebsrat und Betriebsinhaber:in ergeben.

Neben der umfassenden Umschreibung des Überwachungsrechts des Betriebsrates mittels einer Generalklausel werden einzelne Überwachungsbefugnisse durch die beispielshafte Aufzählung (§ 89 Z 1 bis 4 ArbVG) ausgeformt. Nach § 89 Z 1 ArbVG hat der Betriebsrat das Recht, in die von der oder dem Arbeitgeber:in geführten Aufzeichnungen über die Bezüge der Arbeitnehmer:innen und die zur Berechnung dieser Bezüge erforderlichen Unterlagen Einsicht zu nehmen und insbesondere auf ihre Richtigkeit zu überprüfen. Das Recht auf Einsichtnahme in die Lohn- bzw. Gehaltsunterlagen wird auch auf andere die Arbeitnehmer:innen betreffende Aufzeichnungen ausgedehnt, sofern deren Kenntnis für den Betriebsrat zu einer zweckentsprechenden Ausübung seiner betriebsverfassungsrechtlichen Befugnisse nötig ist.

Der Betriebsrat kann diesem gesetzlich normierten Überwachungsrecht wirkungsvoll nur nachkommen, wenn er auch die dazu erforderlichen Informationen bekommt, etwa durch Einsichtnahme in sämtliche abrechnungsrelevante Unterlagen. Eine inhaltliche Einschränkung erfährt das Überwachungsrecht des Betriebsrates insofern, als dem Betriebsrat die Informationen in einem Ausmaß

zur Verfügung zu stellen sind, wie sie für die Ausübung seiner (Pflicht)Befugnisse notwendig sind (OGH 30.10.2017, 9 ObA 115/17b).

Hinzuweisen ist auf die strenge Verschwiegenheitspflicht nach § 115 ArbVG, der der Betriebsrat und dessen Mitglieder unterliegen. Eine Weitergabe oder Veröffentlichung von Daten einzelner Arbeitnehmer:innen ist unzulässig (OGH 17.09.2014, 6 ObA 1/14m).

Beispiel:
Der Betriebsrat ist aufgrund seines nach § 89 ArbVG eingeräumten Überwachungsrechts befugt, die richtige Anrechnung der Vordienstzeiten durch die bzw. den Arbeitgeber:in zu überprüfen. Die dazu erforderlichen Informationen hat die bzw. der Arbeitgeber:in durch Einsicht in die dazu nötigen Unterlagen zu gewähren.

4.2.2 Informationsrechte

Auskunftspflicht der Arbeitgeberin bzw. des Arbeitgebers nach § 91 Abs 1 ArbVG

Gemäß § 91 Abs 1 ArbVG ist die bzw. der Betriebsinhaber:in verpflichtet, dem Betriebsrat auf Anfrage über alle Angelegenheiten, welche die wirtschaftlichen, sozialen, gesundheitlichen oder kulturellen Interessen der Arbeitnehmer:innen des Betriebes berühren, Auskunft zu erteilen.

Der Gesetzgeber hat erkannt, wie bedeutend die Information für eine effektive Interessenvertretung der Arbeitnehmer:innenschaft ist, und hat dem Betriebsrat daher weitgehende Informationsrechte im ArbVG eingeräumt. Zweck der Informationsrechte ist es, der Belegschaft zu ermöglichen, auf betriebliche Entwicklungen zu reagieren, diesbezügliche Auswirkungen abzuklären und Vorschläge zu erstatten. Insbesondere sollen Arbeitgeber:innen nicht aus Überraschungseffekten, Zeitnot, Desorientierung der Arbeitnehmer:innen oder auch „vollendeten Tatsachen" Vorteile ziehen können. Die Information muss die Thematik vollstän-

dig abhandeln und aufschlussreich sein, und sie muss für den jeweiligen Zusammenhang rechtzeitig erfolgen.

Zu beachten ist, dass nach der Judikatur des OGH kein uneingeschränktes, sondern nur ein konkretes, Arbeitnehmer:inneninteressen betreffendes Auskunftsrecht des Betriebsrates besteht: Die Angelegenheit muss geeignet sein, Auswirkungen auf die o. a. Interessen der Arbeitnehmer:innen zu haben, es muss eine ausreichende und aktuelle Beziehung zu den Arbeitnehmer:inneninteressen gegeben sein. Die Auskunftspflicht der Arbeitgeberin bzw. des Arbeitgebers des § 91 Abs 1 ArbVG entsteht bei entsprechend konkretem Verlangen des Betriebsrates (dies ist am besten nachweislich schriftlich zu übermitteln). Die Konkretheit der Anfrage beeinflusst die Informationspflicht der Arbeitgeberin bzw. des Arbeitgebers: Je mehr die Anfrage spezifiziert ist, desto genauer muss die Information sein. Der Betriebsrat kann, wenn die bzw. der Arbeitgeber:in trotz konkreter Nachfrage hierzu keine befriedigende Antwort gibt, das Auskunftsrecht mittels Klage gemäß § 50 Abs 2 ASGG beim zuständigen Arbeits- und Sozialgericht durchsetzen (OGH 22.10.2010, 9 ObA 135/09g).

Beispiel:
„Qualitätsberichte" oder anonyme Mitarbeiter:innenbefragungen kommen in Betrieben immer wieder vor. Anhand der mittels des allgemeinen Auskunftsrechts gewonnenen Informationen kann der Betriebsrat überprüfen, ob nicht allenfalls doch eine zustimmungspflichtige Maßnahme (etwa eine die Menschenwürde berührende Kontrollmaßnahme nach § 96 Abs 1 Z 3 ArbVG) der Arbeitgeberin bzw. des Arbeitgebers vorliegt bzw. ob nicht doch personenbezogene Daten aufgenommen werden.

Informationspflicht der Arbeitgeberin bzw. des Arbeitgebers nach § 91 Abs 2 ArbVG

Ein echtes Informationsrecht des Betriebsrates besteht bei der Verarbeitung von personenbezogenen Beschäftigtendaten: Gemäß § 91 Abs 2 ArbVG haben Arbeit-

geber:innen dem Betriebsrat von sich aus Mitteilung zu machen, welche Arten von personenbezogenen Arbeitnehmer:innendaten automationsunterstützt aufgezeichnet werden und welche Verarbeitungen und Übermittlungen vorgesehen sind.

„Verarbeiten" ist in diesem Zusammenhang weit zu verstehen und umfasst dabei das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten (vgl Art 4 Z 2 DSGVO).

Die Mitteilungspflicht bezieht sich auf die vorgesehene Verarbeitung, sohin auf die in der technischen Gestaltung zum Ausdruck kommenden Absichten bzw. Möglichkeiten der Arbeitgeberin bzw. des Arbeitgebers (und nicht nur auf die tatsächlich vorgenommene Verwendung der Daten!) und umfasst auch spätere Erweiterungen des eingesetzten Systems.

Personenbezug liegt vor, wenn Personen unmittelbar namentlich oder etwa per Personalnummer bezeichnet werden oder wenn ihre Identität bestimmbar ist (was beispielsweise der Fall ist, wenn die erfasste Personengruppe so klein oder eines oder mehrere der erfassten Merkmale so unterscheidungskräftig sind, dass ein Rückschluss auf einzelne Personen dennoch möglich ist). Personenbezogene Daten können beispielsweise Name, Geburtsdatum, Adresse, Sozialversicherungsnummer sein, aber auch Bilddaten, Bewertungen, Standortdaten etc. Nach Art 4 Z 1 DSGVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen".

Zusätzlich ist dem Betriebsrat auf Verlangen die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung von personenbezogenen Daten zu ermöglichen, beispielsweise durch Übergabe von Programmdokumentationen oder Systembeschreibungen etc.

Einsicht in konkrete Daten einzelner Arbeitnehmer:innen hat der Betriebsrat, sofern dies nach § 89 ArbVG oder anderen Rechtsvorschriften erlaubt ist oder die bzw. der betroffene Arbeitnehmer:in zustimmt (siehe dazu oben). Die Befugnisse

des Betriebsrates sollen durch diese Regelung nicht eingeschränkt werden. Der Betriebsrat ist daher berechtigt, gemäß § 89 Z 1 ArbVG in Lohn- und Gehaltslisten, Arbeitszeit- und Urlaubsaufzeichnungen der Arbeitnehmer:innen Einsicht zu nehmen. Ebenso wird keine Zustimmung einzelner Arbeitnehmer:innen erforderlich sein, soweit die Überprüfung der Einhaltung des für den Betrieb geltenden Kollektivvertrages, sonstiger Vorschriften oder etwa der im Betrieb abgeschlossenen Betriebsvereinbarungen eine Einsichtnahme (auch) in bestimmte Daten einzelner Arbeitnehmer:innen im Interesse der Belegschaft erforderlich macht (vgl *Grünanger/Goricnik*, Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle², 30). Über den Inhalt der Aufzeichnungen ist Verschwiegenheit zu wahren!

Fazit:

Der Betriebsrat kann sich nach § 91 Abs 2 ArbVG genaue Kenntnis darüber verschaffen, welche Beschäftigtendaten aufgezeichnet werden, zu welchem Zweck deren Aufzeichnung bzw Verwendung erfolgt und welche Verknüpfungs-, Auswertungs- oder Verarbeitungsmöglichkeiten durch den Einsatz der jeweiligen Systeme möglich sind.

Zu den Überwachungsbefugnissen und Informationsrechten des Betriebsrates siehe ausführlich Auer-Mayer in *Gahleitner/Mosler*, Arbeitsverfassungsrecht 3, 6. Auflage (2020), §§ 89 und 91.

4.2.3 Betriebsvereinbarungstatbestände

Damit beim Umgang mit personenbezogenen Daten im Betrieb die Interessen der Beschäftigten gewahrt werden, hat der Gesetzgeber im ArbVG unterschiedliche Betriebsvereinbarungstatbestände zur Verfügung gestellt.

In den §§ 96 und 96a ArbVG ist angeführt, welche Systeme bzw. Maßnahmen, die personenbezogenen Daten von Arbeitnehmerinnen und Arbeitnehmern ermitteln und weiterverarbeiten, nur nach Abschluss einer Betriebsvereinbarung eingesetzt werden dürfen. Fällt ein System weder unter § 96 ArbVG noch unter § 96a ArbVG,

kann unter Umständen eine Betriebsvereinbarung nach § 97 ArbVG abgeschlossen werden.

Der rechtspolitische Zweck der Regelungen der §§ 96 und 96a ArbVG ist es nicht, Maßnahmen der Arbeitgeberin bzw. des Arbeitgebers zu blockieren oder gar zu verhindern, sondern der Belegschaft (vertreten durch den Betriebsrat) eine starke Verhandlungsposition zu geben: Das Ziel einer Betriebsvereinbarung vor Einsatz einer Maßnahme oder vor Inbetriebnahme des Systems liegt in der präventiven Kontrolle und Sicherstellung der Wahrung der Rechte der Beschäftigten. Der Betriebsrat ist daher von der bzw. dem Arbeitgeber:in rechtzeitig (d. h. bereits in der Planungsphase) zu informieren und miteinzubeziehen, sodass er die berechtigten Arbeitnehmer:inneninteressen noch einbringen kann. In der Betriebsvereinbarung sind die näheren Bedingungen festzulegen, unter denen die bzw. der Arbeitgeber:in die geplante Maßnahme oder das geplante System einsetzen darf – samt Vorkehrungen, um dem Betriebsrat die Kontrolle der Einhaltung zu ermöglichen (beispielsweise durch Einsichtnahme in Protokolldaten etc.).

Zu beachten ist, dass unter „Einführung" von Maßnahmen und Systemen nach den §§ 96 und 96a ArbVG nicht nur die erstmalige Installierung, sondern auch die Anwendung, Änderung, Umstellung, Anpassung oder Erweiterung bestehender Systeme zu verstehen ist. D. h., selbst wenn sich ein System bereits seit geraumer Zeit in Betrieb befindet, ist – bei Vorliegen der Voraussetzungen – eine Betriebsvereinbarung dazu abzuschließen. Ebenso müssen Arbeitgeber:innen neu mit dem Betriebsrat verhandeln, wenn das System entsprechend verändert werden soll.

Zudem kommt es beim Einsatz der Kontroll-, Informations- oder Kommunikationssysteme darauf an, welche objektive Eignung das konkret zum Einsatz gelangende System hat. Ob ein System tatsächlich seine Möglichkeiten vollkommen ausschöpft oder ob nur Teilbereiche genutzt werden sollen, ist daher gleichgültig (OGH 14.7.2022, 9 ObA 60/22x; OGH 27.05.2004, 8 ObA 97/03b).

Und es kommt dem Betriebsrat die „Pflichtbefugnis" zu, die Einhaltung der jeweils abgeschlossenen Betriebsvereinbarungen auch zu kontrollieren.

Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG

Betriebsvereinbarungen nach § 96 ArbVG

Bei den Tatbeständen des § 96 ArbVG handelt es sich um Fälle der **notwendigen Mitbestimmung** – d. h. eine Maßnahme (oder der Einsatz eines Systems) darf ohne Zustimmung des Betriebsrates in Form einer Betriebsvereinbarung nicht durchgeführt werden. Die Zustimmung des Betriebsrates kann nicht durch die Schlichtungsstelle ersetzt werden. Wird die Betriebsvereinbarung gekündigt, erlischt sie ohne Nachwirkung und die Maßnahme ist sofort einzustellen. Werden solche Maßnahmen oder Systeme ohne Zustimmung des Betriebsrates betrieben, kann dieser beim Arbeits- und Sozialgericht – ggf. zwecks schnellerer Durchsetzung unter Erwirkung einer einstweiligen Verfügung – die Unterlassung der Verwendung und Beseitigung der Maßnahmen bzw. Systeme verlangen.

Personalfragebögen nach § 96 Abs 1 Z 2 ArbVG

Nach § 96 Abs 1 Z 2 ArbVG unterliegt die Einführung von Personalfragebögen, sofern in diesen nicht bloß die allgemeinen Angaben zur Person und Angaben über die fachlichen Voraussetzungen für die beabsichtigte Verwendung der Arbeitnehmerin bzw. des Arbeitnehmers enthalten sind, der Zustimmungspflicht des Betriebsrates. Die Zustimmung des Betriebsrates erfolgt wie oben angeführt in Form einer Betriebsvereinbarung. Zustimmungsfrei sind daher die sogenannten schlichten Fragebögen, die nur allgemeine Angaben zur Person der Arbeitnehmerin bzw. des Arbeitnehmers und den fachlichen Voraussetzungen enthalten (beispielsweise Name, Geburtsdatum, Wohnort, Familienstand, Ausbildungen, Zeugnisse, Qualifikationen). Liegt ein Personalfragebogen vor, der darüber hinausgeht, und wurde keine Betriebsvereinbarung abgeschlossen, so ist die Einführung des Personalfragebogens rechtswidrig und der Betriebsrat kann auf Unterlassung klagen.

Der OGH interpretiert den Begriff „Personalfragebogen" allerdings eng. Es können nur solche Maßnahmen der Betriebsinhaberin bzw. des Betriebsinhabers zustimmungspflichtig sein, die geeignet sind, der bzw. dem Arbeitgeber:in Informationen über persönliche Umstände oder Meinungen einer einzelnen Arbeitnehmerin bzw. eines einzelnen Arbeitnehmers zu verschaffen, an deren Geheimhaltung diese:r ein Interesse haben könnte; anonymisierte Mitarbeiter:innenbefragungen

seien auch ohne Zustimmung des Betriebsrates zulässig: Entscheidend für die Zustimmungspflicht ist, ob die Aktion so angelegt ist, dass die bzw. der Arbeitgeber:in durch sie in den Besitz personenbezogener Daten und Informationen gelangen kann. Nicht von Bedeutung ist, ob die Fragebogenaktion von ihr bzw. ihm oder Dritten ausgegangen ist oder durchgeführt wird (OGH 15.12.2004, 9 ObA 114/04m).

Diese Entscheidung ist sehr kritisch zu betrachten! Die Anonymisierung des Fragebogens macht diesen noch nicht mitbestimmungsfrei: Die Aufgabe des Betriebsrates wird es daher sein, sich Kenntnis vom Inhalt des Fragebogens zu verschaffen (siehe obige Ausführungen zu § 91 Abs 1 ArbVG) und unzulässige bzw. prekäre Fragen zu eliminieren. Zudem ist durch die Kontrolle des Betriebsrates sicherzustellen, dass die Auswertung der erhobenen Befragungsergebnisse tatsächlich auf eine Art und Weise erfolgt, dass die bzw. der Arbeitgeber:in keine personenbezogenen Informationen erhält bzw. die Informationen keine Rückschlüsse auf bestimmte Arbeitnehmer:innen ermöglichen und die bzw. der Betriebsinhaber:in keine Einsicht in die Originalfragebögen nimmt. All das könnte und sollte Inhalt einer Betriebsvereinbarung sein.

Fazit:

Auch anonymisierte Fragebögen werden der Zustimmungspflicht des Betriebsrates unterliegen, etwa wenn aus den gestellten Fragen Ergebnisse gewonnen werden können, die Personen zuordenbar sind (z. B. durch die Art der Erhebung, bei Bewertung von Vorgesetzten usw.). Die Belegschaftsvertretung soll durch Ausübung ihrer Überwachungsrechte sicherstellen, dass die Befragung und Auswertung tatsächlich in einer Art und Weise erfolgt, die Anonymität gewährleistet. Zudem ist es ihre Aufgabe, Fragen zu eliminieren, die die Persönlichkeitsrechte der Arbeitnehmer:innen verletzen.

Kontrollmaßnahmen und technische Systeme zur Kontrolle nach § 96 Abs 1 Z 3 ArbVG

Nach § 96 Abs 1 Z 3 ArbVG bedarf die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer:innen der Zustimmung des Betriebsrates in Form einer Betriebsvereinbarung, wenn diese Maßnahmen die Menschenwürde berühren.

Entscheidend für die Zustimmungspflicht nach § 96 Abs 1 Z 3 ArbVG ist daher, ob die Kontrollmaßnahme die Menschenwürde berührt. Der Gesetzgeber will mit der Anknüpfung an die Menschenwürde erreichen, dass die freie Entfaltung der Persönlichkeit der Arbeitnehmerin und des Arbeitnehmers keinen übermäßigen Eingriffen ausgesetzt ist. Entscheidend für die Zustimmungspflicht ist daher die Intensität der Kontrolle. Dabei sind die Art der Kontrolle (durch Menschen oder durch Technik), die zeitliche Dauer (Stichproben oder permanente Kontrolle), der Umfang der Kontrolle (Verknüpfung verschiedener Daten) und die dabei erfassten Datenarten (Sensibilität) ausschlaggebend (*Löschnigg*, ASoK 2005, 37). Es ist zu prüfen, ob das eingesetzte (Kontroll-)Mittel zum angestrebten Zweck in Relation steht oder ob es eine die Persönlichkeitsrechte weniger beeinträchtigende Alternative – sog. „gelindere Mittel" gibt (OGH 20.12.2006, 9 ObA 109/06d).

Ob und gegebenenfalls unter welchen Voraussetzungen eine sachliche Rechtfertigung der Arbeitgeberin oder des Arbeitgebers für den Einsatz einer Kontrollmaßnahme besteht (z. B. Schutz der Sicherheit und Gesundheit von Personen, Schutz des Eigentums der Arbeitgeberin bzw. des Arbeitgebers), hat der Betriebsrat im Rahmen des Abschlusses der Betriebsvereinbarung zu berücksichtigen und auch die nötigen Schutzmaßnahmen für die Arbeitnehmer:innen vor unverhältnismäßiger Überwachung vorzusehen.

In betriebsratslosen Betrieben dürfen solche Kontrollmaßnahmen nur mit Zustimmung der einzelnen Arbeitnehmer:innen durchgeführt werden, die jederzeit widerrufen werden kann, sofern keine schriftliche Vereinbarung über ihre Dauer getroffen wurde (§ 10 Arbeitsvertragsrechts-Anpassungsgesetz, AVRAG).

Maßnahmen, die die Menschenwürde verletzen, sind – selbst mit Zustimmung des Betriebsrates bzw. der Arbeitnehmerin bzw. des Arbeitnehmers – unzulässig.

Maßnahmen, die die Menschenwürde nicht berühren, sind nicht zustimmungspflichtig, wie etwa eine Zutrittskontrolle bei Betreten des Arbeitsortes (Stechuhr). Allerdings stellt die Anordnung solcher Kontrollen eine Ordnungsvorschrift dar, über die eine Betriebsvereinbarung nach § 97 Abs 1 Z 1 ArbVG abgeschlossen werden kann (aber nicht muss, siehe dazu unten).

Beispiel:
Ein elektronisches Telefonkontrollsystem, das die Nummern der angerufenen Teilnehmer:innen systematisch und vollständig den jeweiligen Nebenstellen zugeordnet erfasst, der Einsatz von sog „Fingerscannern" zur Erfassung der Kommens- und Gehenszeiten oder etwa Alkoholkontrollen, die ohne konkreten Verdacht generell durchgeführt werden, berühren – so urteilte auch der OGH – die Menschenwürde. Sie dürfen nur vorgenommen werden, wenn der Betriebsrat in Form einer Betriebsvereinbarung zustimmt (OGH 13.06.2000, 8 ObA 288/01p; OGH 20.12.2006, 9 ObA 109/06d; OGH 20.03.2015, 9 ObA 23/15w; OGH 22.1.2020, 9 ObA 120/19s; OGH 14.7.2022, 9 ObA 60/22x).

Betriebsvereinbarungen nach § 96a ArbVG

Bei den Tatbeständen des § 96a ArbVG handelt es sich um Fälle der notwendigen, aber ersetzbaren Mitbestimmung. Das bedeutet, dass eine Maßnahme ohne Betriebsvereinbarung nicht durchgeführt werden darf, allerdings kann die Zustimmung des Betriebsrates durch die Schlichtungsstelle ersetzt werden. Der Spruch der Schlichtungsstelle wirkt wie eine Betriebsvereinbarung.

Personaldatensysteme nach § 96a Abs 1 Z 1 ArbVG

Gemäß § 96a Abs 1 Z 1 ArbVG ist für die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Arbeitnehmer:innen, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, der Abschluss einer Betriebsvereinbarung erforderlich. Eine Zustimmung ist nicht erfor-

derlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben.

Es unterliegen daher einerseits nur solche Systeme der Zustimmungspflicht, die über die Ermittlung von allgemeinen Angaben zur Person (z. B. Name, Familienstand, Geburtsdatum) und fachlichen Voraussetzungen (z. B. Ausbildungsweg, Schulabschluss, besondere berufliche Qualifikationen, die zuletzt ausgeübte Tätigkeit etc.) hinausgehen. Dabei ist zu beachten, dass zustimmungsfrei nur die Ermittlung dieser sogenannten „schlichten Arbeitnehmer:innendaten" ist. Werden Arbeitnehmer:innendaten dieser Art in weiterer Folge automationsunterstützt verarbeitet, also insbesondere miteinander oder mit anderen Datenbeständen verknüpft oder übermittelt (d. h. an andere Empfänger:innen weitergegeben oder veröffentlicht), so ist die Zustimmungspflicht wieder gegeben.

Andererseits ist die Zustimmung des Betriebsrates nicht erforderlich, soweit die tatsächliche oder vorgesehene Verwendung dieser Daten über die Erfüllung von Verpflichtungen nicht hinausgeht, die sich aus Gesetz, Kollektivvertrag, Betriebsvereinbarungen oder Arbeitsvertrag ergeben. Es muss daher eine konkrete Verpflichtung der Arbeitgeberin bzw. des Arbeitgebers in einer einschlägigen Rechtsquelle vorgesehen sein, bestimmte Daten in bestimmter Weise zu verwenden. Als Beispiele dafür wären die An- und Abmeldung von Arbeitnehmerinnen und Arbeitnehmern bei der Sozialversicherung, die Errechnung der gesetzlichen Lohnabzüge, die Führung von Arbeitszeitaufzeichnungen (jedoch ohne Auswertungs-, Verknüpfungs- und Gegenüberstellungsfunktionen) oder die Führung von Urlaubsaufzeichnungen nach dem Urlaubsgesetz zu nennen.

Für die Frage der „vorgesehenen Verwendung" ist der Leistungsumfang des konkret eingesetzten Programmpakets entscheidend. Die Beurteilung hat daher anhand des gesamten installierten Systems zu erfolgen, dessen Grundlagen dem Betriebsrat offenzulegen sind (OGH 27.05.2004, 8 ObA 97/03b).

Beispiele:
In der Praxis kommen in den allermeisten Fällen Personalinformationssysteme zur Anwendung, mithilfe derer eine Fülle von Beschäftigtendaten zum Zweck der Personalverwaltung und der rascheren und umfassenderen Personaldisposition miteinander verbunden und ausgewertet werden kann (Personalinformationssysteme). Es wird daher davon auszugehen sein, dass Systeme wie beispielsweise SAP, SAP SuccessFactors, Workday, BMD oder SAGE nicht ohne Betriebsvereinbarung betrieben werden dürfen.

Personalbeurteilungssysteme nach § 96a Abs 1 Z 2 ArbVG

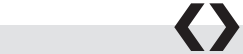
Nach § 96a Abs 1 Z 2 ArbVG bedürfen Systeme zur Beurteilung von Arbeitnehmerinnen und Arbeitnehmern des Betriebes dann der Zustimmung des Betriebsrates, wenn mit diesen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind. Lange Zeit war unklar, was mit dem gesetzlichen Begriff „durch die betriebliche Verwendung gerechtfertigt" gemeint ist. Nach Auslegung des OGH hat dazu ein Interessenvergleich zwischen dem Persönlichkeitsrecht der Arbeitnehmerin bzw. des Arbeitnehmers einerseits und den konkreten betrieblichen Interessen andererseits stattzufinden. Die Abwägung hat aufgrund der konkreten Umstände des Einzelfalles zu erfolgen (OGH 20.08.2008, 9 ObA 95/08y).

Genaue Aussagen, wann nun konkret ein Personalbeurteilungssystem zustimmungsfrei ist, können nicht getroffen werden. Auf die im Einzelfall freiwillige Teilnahme an den Tests durch die Arbeitnehmer:innen kommt es dabei nicht an (OGH 27.02.2018, 9 ObA 94/17i). Tendenziell wird eher dann von einer Mitbestimmungspflicht auszugehen sein, wenn sich die Beurteilung auf künftige (und nicht bereits unmittelbar bevorstehende) Verwendungen bezieht, die Beurteilungskriterien schwer messbar sind oder sich schwerwiegende Konsequenzen an die Beurteilung knüpfen; maßgeblich ist auch, wie die Informationen ermittelt bzw. weiterverwendet werden.

Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG

Zweck des Mitwirkungsrechtes des Betriebsrates ist somit vor allem, durch die Einbringung der (individuellen und kollektiven) Arbeitnehmer:inneninteressen zur Objektivierung des Beurteilungssystems und -verfahrens beizutragen. Eine Betriebsvereinbarung soll die Transparenz von Beurteilungssystemen für Arbeitnehmer:innen erhöhen und damit Manipulationen hintanhalten.

Neben der Beurteilung der Zustimmungspflicht des Betriebsrates nach der Z 2 des § 96a Abs 1 ArbVG ist auch zu fragen, ob nicht noch andere Betriebsvereinbarungstatbestände infrage kommen: So können Personalbeurteilungen u. U. nach § 96 ArbVG (Personalfragebogen, Kontrollmaßnahme) absolut zustimmungspflichtig sein oder aber unter die ersetzbare Zustimmung der Z 1 des § 96a Abs 1 ArbVG (Personaldatensystem) fallen, wenn in deren Rahmen automationsunterstützt Daten erhoben bzw. weiter verwendet werden.



Beispiele:

Werden durch „Führungskraft-Beurteilungsbögen" die berufliche Kompetenz, Persönlichkeitskompetenz und Sozialkompetenz der Arbeitnehmerin oder des Arbeitnehmers nicht nur allgemein, sondern bereits im Zusammenhang mit der in Aussicht genommenen und unmittelbar bevorstehenden Tätigkeit abgefragt, die sowohl an die fachliche als auch an die persönliche und soziale Kompetenz besondere Anforderungen stellt, steht sie im überwiegenden Interesse der Arbeitgeberin bzw. des Arbeitgebers und ist ohne Zustimmung des Betriebsrates gerechtfertigt (OGH 20.08.2008, 9 ObA 95/08y).

Anders lautete die Entscheidung des OGH zu einem Persönlichkeitstest: Ein Bewertungsverfahren, bei dem ausschließlich „Soft Skills" wie Neigungen, Interessen und andere Persönlichkeitsmerkmale wie Belastbarkeit, Frustrationstoleranz und höchstpersönliche „Werte", nicht aber „Hard Skills", also die Fachkompetenz, abgefragt werden, berührt massiv die Persönlichkeit der getesteten Personen und ist nicht durch überwiegende berufliche Interessen gerechtfertigt. Der Einsatz eines derartigen Bewertungsverfahrens bedarf daher der Zustimmung des Betriebsrates (OGH 27.02.2018, 9 ObA 94/17i).

Betriebsvereinbarungen nach § 97 ArbVG

Fällt eine Maßnahme oder ein System weder unter § 96 ArbVG noch unter § 96a ArbVG können u. U. die **erzwingbaren Tatbestände des § 97 Abs 1 Z 1 und Z 6 ArbVG** herangezogen werden.

So stellen beispielsweise Kontrollmaßnahmen, die die Menschenwürde nicht berühren (und somit nicht unter § 96 Abs 1 Z 3 ArbVG fallen) und die nicht automationsunterstützt Daten erheben bzw. mit anderen Datensystemen verbunden sind (und somit nicht unter § 96a Abs 1 Z 1 ArbVG fallen), in der Regel **allgemeine Ordnungsvorschriften** dar. Darüber kann eine erzwingbare Betriebsvereinbarung nach § 97 Abs 1 Z 1 ArbVG abgeschlossen werden. Als Beispiele seien etwa Arbeitszeitkontrollen durch Stechuhren oder die Regelung eines betrieblichen „Whistleblowing"-Systems genannt.

Maßnahmen zur zweckentsprechenden Benützung von Betriebsmitteln können durch eine erzwingbare Betriebsvereinbarung nach § 97 Abs 1 Z 6 ArbVG geregelt werden. Unter „Benützung" ist in diesem Zusammenhang sowohl die dienstliche als auch die private Verwendung zu verstehen. Beispielsweise fallen darunter Benützungsvorschriften für (Mobil-)Telefone oder verschiedene Kommunikations-/Informationsdienste (E-Mail, Internetnutzung) am Arbeitsplatz. Diesbezügliche Kontrollmaßnahmen, sofern sie die Menschenwürde berühren, sind aber zustimmungspflichtig nach § 96 Abs 1 Z 3 ArbVG; allenfalls kann auch der Tatbestand des § 96a Abs 1 Z 1 ArbVG (Personaldatenverarbeitungssystem) in Betracht gezogen werden.

Erzwingbar bedeutet, dass die bzw. der Arbeitgeber:in die Maßnahme zwar auch ohne Zustimmung des Betriebsrates setzen kann (etwa durch Weisung oder Regelung im Arbeitsvertrag), wenn der Betriebsrat in weiterer Folge aber seine Mitwirkungsrechte geltend machen möchte, kann er den Abschluss einer Betriebsvereinbarung verlangen. Wenn keine Einigung mit der oder dem Arbeitgeber:in zustande kommt, kann diese über die Schlichtungsstelle erzwungen werden.

Zu den BV-Tatbeständen siehe ausführlich *Felten/Preiss* in *Gahleitner/Mosler*, Arbeitsverfassungsrecht 3, 6. Auflage (2020), §§ 96, 96a und 97.

SKRIPTEN ÜBERSICHT

VÖGB

PRAKTISCHE GEWERKSCHAFTSARBEIT

PGA-1	Sitzungen, die bewegen
PGA-2	Die Betriebsratswahl
PGA-4	Die Zentralbetriebsratswahl
PGA-8	Gender Mainstreaming im Betrieb
PGA-9	Betriebsversammlungen aktiv gestalten
PGA-10	Projektmanagement
PGA-13	Unsere Anliegen im Betrieb durchsetzen
PGA-14	Mobilisierung und Mitgliedergewinnung
PGA-15	Der Betriebsratsfonds

Die einzelnen Skripten werden laufend aktualisiert.

WIRTSCHAFT, RECHT, MITBESTIMMUNG

WRM-1	Unternehmens- und Gesellschaftsrecht
WRM-2	Mitwirkung im Aufsichtsrat
WRM-3	Bilanz- und Gewinn- und Verlustrechnung
WRM-4	Bilanzanalyse
WRM-5	Konzerne wirtschaftlich betrachtet
WRM-6	Mitbestimmung im Konzern und auf EU-Ebene
WRM-7	Umstrukturierungen: Ausgliederungen, Fusionen, Outsourcing & Co
WRM-8	Investition und Finanzierung
WRM-10	Kostenrechnung
WRM-11	Risikomanagement und Controlling
WRM-12	Konzernabschluss und IFRS
WRM-13	Psychologie im Aufsichtsrat
WRM-14	Wirtschaftskriminalität

ÖFFENTLICHKEITSARBEIT

OEA-1	Damit wir uns verstehen
OEA-2	Auf den Punkt gebracht
OEA-3	Social-Media und Social-Web

ARBEIT UND UMWELT

AUW-2	Arbeiten und Wirtschaften in der Klimakrise
AUW-3	Hitze und UV-Strahlung am Brennpunkt Arbeitsplatz

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen:
www.voegb.at/skripten

5 Datenschutzrecht

Die europäische **Datenschutz-Grundverordnung (DSGVO)** ist seit 25. Mai 2018 unmittelbar anwendbar und hat die Datenschutzrichtlinie 95/46/EG aufgehoben. Der genaue Titel lautet: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Damit soll europaweit ein einheitliches Datenschutzrecht gelten, das einerseits personenbezogene Daten schützen und andererseits den freien Datenverkehr sichern soll.

Die DSGVO bedarf grundsätzlich keines weiteren innerstaatlichen Umsetzungsaktes. Da sie aber zahlreiche „Öffnungsklauseln" für den nationalen Gesetzgeber enthält, gibt es neben der DSGVO weiterhin auch ein **Datenschutzgesetz (DSG)** in Österreich. Der genaue Titel lautet: Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).

5.1 Zentrale Begriffe

Das Datenschutzrecht verwendet rechtstechnische Begriffe, die vom normalen Sprachgebrauch abweichen. Hier eine kurze Erklärung:

Personenbezogene Daten: Darunter sind alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. (Art 4 Z 1 DSGVO)

Besondere Kategorien personenbezogener Daten (vormals sensible Daten): Daten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder Gewerkschaftszugehörigkeit hervorgehen, sowie Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung, genetische Daten sowie biometrische Daten. (Art 9 DSGVO)

Verarbeitung: Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang (oder Vorgangsreihe) im Zusammenhang mit personenbezogenen Daten. Dazu zählen etwa das Erfassen, Speichern, Verknüpfen, Ausdrucken, Übermitteln etc. von Daten. (Art 4 Z 2 DSGVO)

Dateisystem: Jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien geordnet ist. (Art 4 Z 6 DSGVO)

Verantwortliche:r: Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. (Art 4 Z 7 DSGVO)

Auftragsverarbeiter:in (vormals Dienstleister:in): Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag der bzw. des Verantwortlichen verarbeitet. (Art 4 Z 8 DSGVO)

5.2 Anwendungsbereich

Auf welche Datenverarbeitung ist das Datenschutzrecht anwendbar:

Sachlich: Der sachliche Anwendungsbereich erstreckt sich auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie auf die nicht automatisierte Verarbeitung personenbezogener Daten, welche in einem Dateisystem gespeichert sind oder gespeichert werden.

Ausgenommen ist die Datenverarbeitung zu ausschließlich persönlichen oder familiären Zwecken, ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit. *(Art 2 DSGVO)*

Örtlich: Es gilt das Marktortprinzip; das europäische Datenschutzrecht gilt somit auch für außereuropäische Unternehmen. Die DSGVO ist anwendbar, wenn die Verarbeitung von einer bzw. einem Verantwortlichen vorgenommen wird, die oder der ihre oder seine Niederlassung in der EU hat – und das unabhängig davon, ob die Verarbeitung von personenbezogenen Daten selbst in der EU stattfindet oder nicht.

Auch wenn ein Unternehmen keine Niederlassung in der EU hat, ist die DSGVO anwendbar, und zwar dann, wenn dieses Unternehmen in der EU aufhältigen Personen Waren oder Dienstleistungen anbietet oder ihr Verhalten beobachtet und in diesem Zusammenhang deren personenbezogene Daten verarbeitet. *(Art 3 DSGVO)*

5.3 Grundsätze der Datenverarbeitung

Bei jeder Verarbeitung von personenbezogenen Daten müssen bestimmte Grundsätze eingehalten werden. Diese bestanden im Wesentlichen schon nach der alten DS-RL und dem DSG 2000:

- Die Daten müssen rechtmäßig, nach Treu und Glauben und transparent (nachvollziehbar) für die bzw. den Betroffene:n verarbeitet werden (Grundsatz der **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**). *(Art 5 Abs 1 lit a DSGVO)*
- Die Verarbeitung erfolgt für genau festgelegte, eindeutige und legitime Zwecke (Grundsatz der **Zweckbindung**). *(Art 5 Abs 1 lit b DSGVO)*
- Die Verwendung ist auf das für die Zwecke ihrer Verarbeitung notwendige Maß zu beschränken (Grundsatz der **Datenminimierung**). *(Art 5 Abs 1 lit c DSGVO)*
- Die Daten müssen sachlich richtig und wenn nötig auf den neuesten Stand gebracht werden (Grundsatz der **Richtigkeit**). *(Art 5 Abs 1 lit d DSGVO)*
- Die Speicherdauer identifizierbarer Personendaten ist auf das unbedingt erforderliche Mindestmaß zu begrenzen (Grundsatz der **Speicherbegrenzung**). *(Art 5 Abs 1 lit e DSGVO)*
- Die Verarbeitung muss Sicherheit und Vertraulichkeit der personenbezogenen Daten gewährleisten, geeignete technische und organisatorische Maßnahmen sind vorzusehen (Grundsatz der **Integrität und Vertraulichkeit**). *(Art 5 Abs 1 lit f DSGVO)*

Neu ist die sogenannte **Rechenschaftspflicht** (Accountability). Das bedeutet, dass die:der Verantwortliche die Einhaltung der Grundsätze nachweisen muss. *(Art 5 Abs 2 DSGVO)*

5.4 Rechtmäßigkeit der Datenverarbeitung

Jede Verarbeitung personenbezogener Daten muss rechtmäßig sein. Das heißt, bei jeder Datenverarbeitung muss sich die bzw. der Verantwortliche auf einen Erlaubnistatbestand stützen können. Folgende Möglichkeiten bestehen:

- Eine Datenverarbeitung ist grundsätzlich dann rechtmäßig, wenn die betroffene Person nachweislich ihre Zustimmung (**Einwilligung**) gegeben hat. *(Art 6 Abs 1 lit a DSGVO)*
- Die Datenverarbeitung ist entweder zur Erfüllung einer **vertraglichen Verpflichtung** gegenüber der betroffenen Person oder zur Erfüllung einer **rechtlichen Pflicht** erforderlich. *(Art 6 Abs 1 lit b und lit c DSGVO)*
- Die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im **öffentlichen Interesse** liegt oder in Ausübung öffentlicher Gewalt erfolgt. *(Art 6 Abs 1 lit e DSGVO)*
- Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder anderer natürlicher Personen zu schützen. *(Art 6 Abs 1 lit d DSGVO)*
- Die Verarbeitung ist zur Wahrung der **berechtigten Interessen** der bzw. des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. *(Art 6 Abs 1 lit f DSGVO)*

5.5 Die Betroffenenrechte

Die Betroffenenrechte stehen in Korrelation mit den Grundsätzen der DSGVO und führen diese näher aus. Durch die DSGVO wurden die Rechte der betroffenen Personen, deren Daten verarbeitet werden, gestärkt:

- Betroffene haben ein **Recht auf transparente Information** bei Erhebung bzw. Verwendung ihrer Daten. *(Art 12, Art 13 und Art 14 DSGVO)*
- Die betroffene Person hat das Recht auf eine Bestätigung, ob sie betreffende personenbezogene Daten verarbeitet werden (**Recht auf Auskunft**). Eine Ko-

pie der Daten, die Gegenstand der Verarbeitung sind, ist von der bzw. dem Verantwortlichen zur Verfügung zu stellen. Dies erste Kopie ist kostenfrei. *(Art 15 DSGVO)*

- Sind Daten unrichtig oder unvollständig, kann eine unverzügliche Berichtigung oder Vervollständigung verlangt werden (**Recht auf Berichtigung**). *(Art 16 DSGVO)*
- Wird die Einwilligung einer betroffenen Person zur Verarbeitung ihrer Daten widerrufen, kann die Löschung dieser Daten verlangt werden (**Recht auf Löschung**). Dieses Recht bzw. das Recht auf Einschränkung der Verarbeitung besteht auch, wenn die Daten für die Verarbeitungszwecke nicht (mehr) notwendig sind. *(Art 17 und Art 18 DSGVO)*
- Verantwortliche haben Betroffene bei der Durchsetzung ihres Löschungsanspruchs gegenüber Dritten zu unterstützen (**Recht auf Vergessenwerden**). *(Art 17 Abs 2 und Art 19 DSGVO)*
- Betroffene können die Herausgabe ihrer Daten zudem in einem Format verlangen, das es ihnen ermöglicht, diese Daten bei einer:einem anderen Anbieter:in weiter zu nutzen (**Recht auf Datenübertragbarkeit**). *(Art 20 DSGVO)*
- Ein Widerspruch gegen die Verarbeitung von personenbezogenen Daten kann eingelegt werden, wenn kein berechtigtes Interesse des Verantwortlichen zur Verarbeitung vorliegt oder Daten ohne öffentliches Interesse zu Forschungs- oder statistischen Zwecken verwendet werden oder Daten zur Direktwerbung verarbeitet werden (**Recht auf Widerspruch**). *(Art 21 DSGVO)*

Die Rechte der Betroffenen wurden auch gestärkt, indem bereits Hersteller:innen und Verantwortliche zu datenschutzfreundlichen Produkten (Prozessen) und Voreinstellungen verpflichtet sind (**Privacy by Design/Privacy by Default**). *(Art 25 DSGVO)*

5.6 Dokumentations- und Nachweispflichten des Verantwortlichen

Auf Unternehmensebene brachte das Datenschutzrecht mit 25. Mai 2018 erweiterte **Dokumentations- und Nachweispflichten**. Die Meldung an das Datenverarbeitungsregister (DVR) ist mit Ablauf des 24. Mai 2018 weggefallen. Die Verantwortlichen müssen selbst die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (etwa Rechtmäßigkeit, Zweckbindung, Transparenz oder Datenminimierung etc.) nachweisen. Der Nachweis wird in der Regel durch eine entsprechende Dokumentation (siehe auch Verzeichnis von Verarbeitungstätigkeiten) erfolgen. *(Art 5 Abs 2 DSGVO)*

Eigens gefordert wird auch die Dokumentation der **getroffenen technischen und organisatorischen Maßnahmen (TOMs)**, die ein Schutzniveau bieten, das dem mit der beabsichtigten Verarbeitung geschaffenen Risiko für die betroffenen Personen angemessen ist. Diese Maßnahmen schließen auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten ein. *(Art 24, Art 25 DSGVO)*

Im Detail geregelt ist zudem die Führung eines **Verzeichnisses von Verarbeitungstätigkeiten**. Dieses hat folgende Informationen zu enthalten:

- Name und Kontaktdaten der bzw. des Verantwortlichen,
- Name und Kontaktdaten der bzw. des Datenschutzbeauftragten (sofern bestellt),
- Zweck€ der Verarbeitung,
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängerinnen und Empfängern,
- gegebenenfalls Übermittlungen personenbezogener Daten in ein Drittland oder an eine internationale Organisation,
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,

» wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

Die Verpflichtung zur Führung eines Verarbeitungsverzeichnisses trifft alle Unternehmen und Einrichtungen, die 250 und mehr Mitarbeiter:innen beschäftigen. Unternehmen und Einrichtungen, die weniger als 250 Mitarbeiter:innen beschäftigen, müssen ebenfalls ein Verarbeitungsverzeichnis führen, wenn die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder die Verarbeitung nicht nur gelegentlich erfolgt oder besondere Kategorien von Daten verarbeitet werden. Das heißt, diese Ausnahme wird in der Praxis nur in wenigen Fällen zutreffen.

Das Verzeichnis ist schriftlich zu führen (allenfalls in einem elektronischen Format) und auf Anfrage der Datenschutzbehörde zur Verfügung zu stellen. *(Art 30 DSGVO)*

Hat eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine **Datenschutz-Folgenabschätzung** durchzuführen. Diese ist insbesondere erforderlich, wenn

» eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und diese als Grundlage für automatisierte Entscheidungen dient, die natürliche Personen in erheblicher Weise benachteiligen können (z. B. Profiling, Bonitätsentscheidungen),

» eine umfangreiche Verarbeitung besonderer Kategorien von Daten (ehemals sensibler Daten) erfolgt oder

» eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche erfolgt.

Die Datenschutzbehörde hat eine Liste von Verarbeitungen erstellt, für die jedenfalls eine Datenschutz-Folgenabschätzung durchzuführen ist („schwarze" Liste), und sie hat zudem eine Liste von Verarbeitungen erstellt, für die keine Datenschutz-Folgenabschätzung erforderlich ist („weiße" Liste). Die Verordnungen da-

zu können auf der Homepage der Datenschutzbehörde abgerufen werden (https://www.dsb.gv.at/rechte-pflichten/rechtsquellen). *(Art 35 DSGVO)*

Bei hohem Risiko besteht eine Pflicht zur **Vorabkonsultation der Datenschutzbehörde**. *(Art 36 DSGVO)*

Verantwortliche müssen daher jederzeit in der Lage sein, die Einhaltung der Vorgaben für die Datenverarbeitungen sowohl in rechtlicher wie in technischer und organisatorischer Sicht nachweisen zu können. Eine fehlende Dokumentation kann zu empfindlichen Bußgeldern führen.

5.7 Die bzw. der Datenschutzbeauftragte

Die Benennung von Datenschutzbeauftragten ist nun verpflichtend vorgesehen, und zwar bei allen öffentlichen und nicht-öffentlichen Stellen, bei denen besonders risikoreiche Datenverarbeitungen erfolgen. Das ist der Fall, wenn

» deren Kerntätigkeit eine umfangreiche, regelmäßige und systematische Beobachtung der betroffenen Personen erforderlich macht oder

» wenn deren Kerntätigkeit die Verarbeitung besonderer Kategorien von Daten betrifft.

Die Mitgliedstaaten haben zudem die Möglichkeit, eine weitergehende Bestellpflicht einzuführen. Davon wurde im DSG kein Gebrauch gemacht. Den Unternehmen ist es allerdings unbenommen, freiwillig eine:n Datenschutzbeauftragte:n zu benennen.

Die bzw. der Datenschutzbeauftragte benötigt eine entsprechende Qualifikation und Fachwissen, sie bzw. er ist in ihrer bzw. seiner Funktion weisungsfrei, darf wegen dieser Tätigkeit nicht abberufen oder benachteiligt werden und unterliegt einer Verschwiegenheitspflicht. *(Art 37, Art 38 DSGVO)*

Die für die betriebliche Ebene **wichtigsten Aufgaben** der bzw. des Datenschutzbeauftragten bestehen darin:

» die Betroffenen zu unterrichten und ihnen Auskunft zu erteilen,

» das Einhalten des Datenschutzrechts zu überwachen (z. B. die Abhaltung von Schulungen für Mitarbeiter:innen),

» die Verantwortlichen (die Unternehmensführung) zu unterstützen,

» der höchsten Managementebene zu berichten,

» mit der Behörde zusammenzuarbeiten, insbesondere i. Z. m. der Datenschutz-Folgenabschätzung *(Art 39 DSGVO)*

5.8 Die Datenschutzbehörde (= Aufsichtsbehörde)

Die Datenschutzbehörde sorgt für die Einhaltung des Datenschutzes in Österreich. Sie ist in Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig und daher weisungsfrei und zur Verschwiegenheit verpflichtet.

Die Datenschutzbehörde hat eine **Vielzahl an Aufgaben**, wesentliche davon sind:

» Überwachung und Durchsetzung der DSGVO,

» Sensibilisierung und Aufklärung der Öffentlichkeit[5], Sensibilisierung der Verantwortlichen und Auftragsverarbeiter,

» Beratung des Parlaments, der Regierung und Gremien,

» Befassung mit Beschwerden einer betroffenen Person oder einer sie vertretenden Stelle oder Organisation,

» Zusammenarbeit mit anderen Aufsichtsbehörden,

» Untersuchungen über die Anwendung dieser Verordnung durchführen, Entwicklungen verfolgen,

» Festlegung von Standardvertragsklauseln, Liste der Verarbeitungen erstellen, für die eine Datenschutz-Folgenabschätzung erforderlich ist, Ausarbeitung

von Verhaltensregeln fördern, Aufgaben im Zusammenhang mit Zertifizierungsmechanismen usw. *(Art 51 ff, Art 57 DSGVO, § 21 DSG)*

Um die Aufgaben erfüllen zu können, werden der Datenschutzbehörde **umfangreiche Befugnisse** eingeräumt. Diese umfassen Untersuchungsbefugnisse, wie etwa Einsicht in Datenverarbeitungen und Unterlagen, bei der die bzw. der Verantwortliche bzw. Auftragsverarbeiter zur Mitwirkung und Unterstützung verpflichtet ist und sogenannte Abhilfebefugnisse. Damit kann die Behörde rechtswidriges Verhalten beenden. Sie kann Warnungen oder Verwarnungen aussprechen, Anweisungen erteilen, rechtswidrige Verarbeitungsvorgänge zu unterlassen oder sogar Verarbeitungen beschränken oder verbieten. Dazu kommen Genehmigungsbefugnisse und Beratungsbefugnisse. *(Art 55, Art 58 DSGVO, § 22 DSG)*

Bei grenzüberschreitenden Fällen steht den Unternehmen die Datenschutzbehörde an ihrem Hauptsitz als Ansprechpartner zur Verfügung. Betroffene Personen können sich bei Beschwerden an die Datenschutzbehörde ihres Wohnsitzstaates wenden, die den Sachverhalt (wenn er grenzüberschreitend ist) mit den übrigen betroffenen Datenschutzbehörden unter Federführung der Datenschutzbehörde am Hauptsitz des Unternehmens klärt. *(Art 56, Art 60 ff DSGVO)*

5.9 Rechtsbehelfe und Sanktionen

Bei Verletzungen des Datenschutzrechts hat eine betroffene Person Anspruch auf Unterlassung und Beseitigung des rechtswidrigen Zustands:

- Dazu kann jede betroffene Person eine Beschwerde bei der Datenschutzbehörde einbringen.
- Gegen Bescheide der Datenschutzbehörde und gegen Untätigkeit der Datenschutzbehörde kann eine Bescheidbeschwerde bzw. Säumnisbeschwerde an das Bundesverwaltungsgericht (BVwG) gerichtet werden.
- Jede betroffene Person kann wahlweise auch einen gerichtlichen Rechtsbehelf ergreifen *(Art 77 ff DSGVO, §§ 24 ff DSG)*

Betroffene können auch Schadenersatzansprüche geltend machen: Es ist der materielle (erlittene) und immaterielle Schaden (Entschädigung für die erlittene Kränkung) zu ersetzen; zuständig ist das Landesgericht für Zivilrechtssachen, in dessen Sprengel die bzw. der Kläger:in ihren bzw. seinen gewöhnlichen Aufenthalt hat (allenfalls auch am Aufenthaltsort des Beklagten).

Daneben kommt den Datenschutzbehörden (= Aufsichtsbehörden) auch Strafbefugnis zu: Je nach Art des Datenschutzverstoßes können Geldbußen verhängt werden

» von bis zu Euro 10.000.000 oder im Falle eines Unternehmens bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (z. B. bei einem Verstoß gegen die Bestimmungen über die Führung eines Verzeichnisses von Verarbeitungstätigkeiten, die Bestimmungen zur Datenschutz-Folgenabschätzung etc.);

» von bis zu Euro 20.000.000 oder im Fall eines Unternehmens bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs (z. B. bei einem Verstoß gegen die Grundsätze der Verarbeitung, Rechte der betroffenen Personen, Bestimmungen zur Datenübermittlung an Drittstaaten, Nichtbefolgung von Anweisungen der Datenschutzbehörde etc.). *(Art 82 f DSGVO)*

Die Höhe der Geldbuße hängt u. a. von der Art, Schwere und Dauer des Datenschutzverstoßes und vom Verschulden (Vorsatz, Fahrlässigkeit) ab.

» In Österreich kann die Datenschutzbehörde daneben für bestimmte Verstöße eine Verwaltungsstrafe von bis zu Euro 50.000 verhängen (z. B. für das vorsätzliche widerrechtliche Verschaffen eines Zugangs zu einer Datenverarbeitung etc.). *(§ 62 DSG)*

Die Datenschutzbehörde soll bei der Anwendung des Strafenkatalogs die „Verhältnismäßigkeit" wahren und so bei erstmaligen Verstößen von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen. *(§ 11 DSG)*

Die Verwendung von personenbezogenen Daten in Gewinn- oder Schädigungsabsicht ist ein gerichtlich strafbarer Tatbestand. *(§ 63 DSG)*

5.10 Betriebsrat/Betriebsvereinbarungen und Datenschutz

Eine Öffnungsklausel in Artikel 88 DSGVO „Datenverarbeitung im Beschäftigungskontext" ermöglicht es den Mitgliedstaaten im Bereich des Beschäftigtendatenschutzes „spezifischere" Vorschriften durch eigene Rechtsvorschriften vorzusehen. Daneben kommen diesbezüglich auch Kollektivvereinbarungen in Betracht, darunter sind nach Erwägungsgrund 155 auch Betriebsvereinbarungen zu verstehen. Derartige Regelungen können für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrages oder der Beendigung des Beschäftigungsverhältnisses getroffen werden. Der EuGH hat aber klargestellt, dass nationale Rechtsvorschriften oder Kollektivvereinbarungen (einschließlich Betriebsvereinbarungen), die auf Art 88 Abs 1 DSGVO basieren, nicht nur die Anforderungen von Art 88 Abs 2 DSGVO (angemessene und besondere Maßnahmen zur Wahrung der Menschenwürde) erfüllen müssen, sondern auch die allgemeinen Bestimmungen der DSGVO, insb. Art 5, Art 6 Abs 1 sowie Art 9 Abs 1 und 2 DSGVO. Dies bedeutet, dass Betriebsvereinbarungen als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext stets im Einklang mit den Grundsätzen der DSGVO stehen müssen (EuGH 19.12.2024, C-65/23).

Hinzuweisen ist, dass generell die Vorschriften der DSGVO und des DSG (z. B. die allgemeinen Grundsätze der Datenverarbeitung, die Zulässigkeit einer konkreten Datenverwendung, die Rechte der betroffenen Personen, weitere datenschutzrechtliche Verpflichtungen der bzw. des Verantwortlichen, wie Datensicherheitsmaßnahmen, Geheimnisschutz) selbstverständlich auch im Arbeitsverhältnis gelten.

Mitwirkungsbefugnisse nach dem ArbVG sowie § 10 AVRAG: Hervorzuheben sind weiters die Regelungen in arbeitsrechtlichen Vorschriften, wie etwa die Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG (§§ 89 ff ArbVG, siehe dazu oben) oder auch § 10 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG), der den Einsatz von Kontrollmaßnahmen, die die Menschenwürde berühren, in betriebsratslosen Betrieben an die Zustimmung der Arbeitnehmerin bzw. des Arbeitnehmers bindet.

6 Gestaltungsansätze (Rahmen-BV, BV)

6.1 Frageliste zu IT-Systemen

Um zu einem ersten Überblick der im eigenen Unternehmen zum Einsatz kommenden IT-Systeme zu gelangen, empfiehlt es sich, der bzw. dem Arbeitgeber: in folgende Fragen zu stellen.

Die bzw. der Arbeitgeber:in ist, wie oben im Kapitel 4 „Arbeitsverfassung" zu den Informationspflichten nach § 91 Abs 2 ausgeführt, zur umfassenden Beantwortung dieser Fragen verpflichtet. Sie bzw. er kann dabei auf die datenschutzrechtliche Dokumentation, die aufgrund der Anforderungen der DSGVO vorliegen muss, zurückgreifen und diese gegebenenfalls noch ergänzen.

Folgende Fragen können für **JEDES** Informationssystem (IT-Systeme), das im Unternehmen personenbezogene Beschäftigtendaten verarbeitet, gestellt werden:

- Welche Bezeichnung hat das eingesetzte/geplante IT-System, wer ist der Anbieter?
- In welcher Form liegt eine technische Beschreibung des IT-Systems vor?
- Handelt es sich bei diesem System um eine Cloud-Anwendung?
- Für welche(n) Verarbeitungszweck€ soll das IT-System eingesetzt werden?
- Welche datenschutzrechtliche Dokumentation liegt zu diesem IT-System vor?
- Welche Datenarten sollen verarbeitet werden und wie lange werden diese Daten gespeichert?
- Welche personenbezogenen Auswertungen sind möglich und welche sind geplant?
- Werden nur Standauswertungen zur Verfügung gestellt oder können die Benutzer:innen auch eigene Auswertungen flexibel gestalten?
- Sind Datenübermittlungen vom IT-System zu anderen IT-Systemen geplant (Beschreibung der technischen Schnittstellen oder Downloadmöglichkeit, z. B. in Excel)?

» Werden personenbezogene Daten an Dritte (andere Konzernteile, Auftragsverarbeiter:innen, ...) übermittelt bzw. diesen zur Verfügung gestellt und auf Basis welcher Rechtsgrundlage beruht dieser Datentransfer?

» Welche Rollen und Berechtigungen sieht das IT-System vor (Beschreibung des Berechtigungskonzepts/der Rollenbeschreibung), d. h. wer hat Zugriff auf die Daten und Funktionen?

» Welche technischen und organisatorischen Maßnahmen zur Datensicherheit (TOMs) sind geplant bzw. wurden bereits ergriffen?

Zusätzlich zu diesen Fragen kann im Hinblick auf die Verwendung von KI-Systemen weiters hinterfragt werden:

» Gibt es aktuell KI-Systeme oder IT-Systeme mit KI-Funktionalität im Unternehmen?

» Welche Pläne gibt es zum Ausbau/zur Einführung von KI-Systemen?

» Welche technischen und organisatorischen Maßnahmen zum Umgang mit KI-Systemen sind geplant bzw. wurden bereits umgesetzt (z. B. KI-Richtlinie)?

Auf Grundlage der Antworten kann dann vom Betriebsrat abgeschätzt werden, welche Regelung (z. B. Abschluss einer Betriebsvereinbarung) für ein konkretes IT-System erforderlich ist und welche (inner- und außer-)betriebliche Unterstützung der Betriebsrat dazu benötigt.

6.2 „Spielregeln" für die Verarbeitung personenbezogener Mitarbeiter:innendaten – Die Rahmen-Betriebsvereinbarung

Die umfassenden technischen, organisatorischen und rechtlichen Anforderungen, die die DSGVO und seit kurzem die KI-Verordnung mit sich bringen, und die bestehenden Mitwirkungsrechte des Betriebsrats nach dem ArbVG können als Basis dienen, um den Umgang mit Beschäftigtendaten im Besonderen und die betriebliche Datenschutzkultur im Allgemeinen „unter die Lupe zu nehmen". Um diesen Prozess strukturiert und qualitätsgesichert zu unterstützen, hat sich in Deutschland und Österreich, zwei Staaten, die eine ähnliche Form der Mitwirkung und -gestaltung des Betriebsrates in ihrem Arbeitsrecht kennen, der Ab-

schluss einer sogenannten Rahmen-Betriebsvereinbarung zur personenbezogenen Datenverarbeitung vor allem in größeren Unternehmen bewährt.

So können sich die betrieblichen Vertragsparteien bereits im Vorfeld darauf verständigen, welche Fragen zwischen Arbeitgeber:in und Betriebsrat unabhängig vom eingesetzten System geregelt werden können, quasi als Spielregel für die in Folge stattfindende Regelung der unterschiedlichen Systeme.

Bei der Durchsicht abgeschlossener Betriebsvereinbarungen zu einzelnen Systemen zeigt sich, dass diese Vereinbarungen zwei große Regelungsbereiche aufweisen: Zum einen werden technische Aspekte zum konkreten System geregelt, wie z. B. welche Daten erfasst und ausgewertet werden dürfen, welche Zugriffsrechte vorgesehen sind, an welche Drittsysteme personenbezogene Daten übermittelt werden und inwiefern auf Basis einer Protokollierung festgestellt werden kann, welche Verarbeitungsschritte von welchen Nutzerinnen und Nutzern vorgenommen werden. Diese Fragen können für jedes technische System nur spezifisch beantwortet und vereinbart werden, da diese Systeme über unterschiedliche Möglichkeiten zur Verarbeitung von Daten verfügen (man spricht dabei von Funktionalität). Zum anderen finden sich in Vereinbarungen organisatorische Regelungen, z. B. in welcher Form der Betriebsrat informiert und in Änderungsprozesse einbezogen wird, welche Rechte und Pflichten die Beschäftigten besitzen, deren Daten verarbeitet werden, und wie Auftragsverarbeiter:innen vertraglich zu verpflichten sind. Diese organisatorischen Regelungspunkte ähneln sich in vielen Vereinbarungen.

Gelingt es nun, diese organisatorischen Regelungen einmal und in Hinblick auf alle gegenwärtigen und zukünftigen IT-Systeme zu vereinbaren, ersparen sich Arbeitgeber:in und Betriebsrat, dies für jede Einzelvereinbarung neu zu verhandeln. Dieses Ziel verfolgt die Rahmen-Betriebsvereinbarung! Sie stellt als Rahmenvereinbarung allgemeine Regeln im Umgang mit personenbezogenen Daten auf und gilt umfassend für alle bereits im Unternehmen eingesetzten und alle zukünftigen Systeme. Für eine Vielzahl an IT-Systemen, die nur wenige personenbezogene Daten verarbeiten, werden diese Regelungen ausreichend sein. Für einzelne Systeme mit einer Vielzahl an personenbezogenen Daten und darauf auf-

bauenden Möglichkeiten zur Auswertung/Analyse dieser Daten sind dann jeweils spezifische technische Details als Zusatz-Betriebsvereinbarung auszuhandeln.

6.3 Betriebsvereinbarungen für konkrete IT-Systeme

Für konkrete IT-Systeme, die personenbezogene Mitarbeiter:innendaten verarbeiten, kann nach Abschluss der Rahmen-Betriebsvereinbarung somit, wie in Folge beschrieben, verfahren werden.

In der Praxis haben sich drei Wege als praktikabel herausgestellt:

Zum einen wird es IT-Systeme mit einer sehr allgemeinen Verarbeitung von personenbezogenen Daten geben, für die die Regelungen der Rahmen-Betriebsvereinbarung ausreichend sind.

Zum anderen wird bei IT-Systemen, die eine umfangreichere Verarbeitung von personenbezogenen Daten vorsehen, z. B. mit Kontrollmaßnahmen, der Abschluss einer (Zusatz-)Betriebsvereinbarung notwendig sein. Als Zwischenlösung könnte auch ein Datenblatt mit der Beschreibung des Ist-Standes, d. h. der datenschutzrechtlichen Dokumentation, beigefügt werden. Dieses Datenblatt sollte zumindest folgende Regelungspunkte ansprechen:

- Bezeichnung IT-System,
- Zweck der Datenverarbeitung,
- (optional) Nichtziel,
- personenbezogene Daten,
- vereinbarte personenbezogene Auswertungen und Analysen,
- Übermittlung der erzeugten Daten in andere Systeme (Beschreibung Schnittstelle),
- Übermittlung von Daten an betriebsexterne Empfänger:innen,
- Rollen- und Berechtigungskonzept,
- (optional) organisatorische Regeln (technische organisatorische Maßnahmen TOMs).

6 Gestaltungsansätze (Rahmen-BV, BV)

Zuallerletzt wird es vielleicht schon Betriebsvereinbarungen zu einzelnen IT-Systemen geben; diese können beibehalten oder im Hinblick auf die Regelungen der Rahmen-Betriebsvereinbarung neu verhandelt werden.

SKRIPTEN ÜBERSICHT

VÖGB

SOZIALRECHT

SR-1	Grundbegriffe des Sozialrechts
SR-2	Sozialpolitik im internationalen Vergleich
SR-3	Sozialversicherung – Beitragsrecht
SR-4	Pensionsversicherung I: Allgemeiner Teil
SR-5	Pensionsversicherung II: Leistungsrecht
SR-6	Pensionsversicherung III: Pensionshöhe
SR-7	Krankenversicherung I: Allgemeiner Teil
SR-8	Krankenversicherung II: Leistungsrecht
SR-9	Unfallversicherung
SR-10	Arbeitslosenversicherung I: Allgemeiner Teil
SR-11	Arbeitslosenversicherung II: Leistungsrecht
SR-12	Insolvenz-Entgeltsicherung
SR-13	Finanzierung des Sozialstaates
SR-14	Pflege und Betreuung

Die einzelnen Skripten werden laufend aktualisiert.

ARBEITSRECHT

AR-1	Kollektive Rechtsgestaltung
AR-2A	Betriebliche Interessenvertretung
AR-2B	Mitbestimmungsrechte des Betriebsrates
AR-2C	Rechtstellung des Betriebsrates
AR-3	Arbeitsvertrag
AR-4	Arbeitszeit
AR-5	Urlaubsrecht
AR-6	Entgeltfortzahlung im Krankheitsfall
AR-7	Gleichbehandlung im Arbeitsrecht
AR-8A	ArbeitnehmerInnenschutz I: Überbetrieblicher ArbeitnehmerInnenschutz
AR-8B	ArbeitnehmerInnenschutz II: Innerbetrieblicher ArbeitnehmerInnenschutz
AR-9	Beendigung des Arbeitsverhältnisses
AR-10	Arbeitskräfteüberlassung
AR-11	Betriebsvereinbarung
AR-12	Lohn(Gehalts)exekution
AR-13	Berufsausbildung
AR-14	Wichtiges aus dem Angestelltenrecht
AR-15	Betriebspensionsrecht I
AR-16	Betriebspensionsrecht II
AR-18	Abfertigung neu
AR-19	Betriebsrat – Personalvertretung Rechte und Pflichten
AR-21	Atypische Beschäftigung
AR-22	Die Behindertenvertrauenspersonen

GEWERKSCHAFTSKUNDE

GK-1	Was sind Gewerkschaften? Struktur und Aufbau der österreichischen Gewerkschaftsbewegung
GK-2	Geschichte der österreichischen Gewerkschaftsbewegung von den Anfängen bis 1945
GK-3	Die Geschichte der österreichischen Gewerkschaftsbewegung von 1945 bis heute
GK-4	Statuten und Geschäftsordnung des ÖGB
GK-5	Vom 1. bis zum 19. Bundeskongress
GK-7	Die Kammern für Arbeiter und Angestellte
GK-8	Die sozialpolitischen Errungenschaften des ÖGB
GK-9	Geschichte der Kollektivverträge

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen:
www.voegb.at/skripten

7 Der AI Act

Zusätzlich zu den bisher beschriebenen rechtlichen Rahmenbedingungen bei der Verarbeitung von personenbezogenen Daten, sind nun auch die Anforderungen der KI-Verordnung (AI Act) betrieblich zu prüfen.

Wobei hier festzuhalten ist, dass die Diskussion rund um Künstliche Intelligenz nicht neu ist, sondern schon seit über 70 Jahren besteht.

Eine der ersten Zuschreibungen der technischen Möglichkeiten der Künstlichen Intelligenz stammt aus dem August 1955, als Expertinnen und Experten die Annahme aufstellten[6], dass jeder Aspekt des Lernens oder jedes andere Merkmal der Intelligenz prinzipiell so genau beschrieben werden kann, dass eine Maschine dazu gebracht werden kann, es zu simulieren.

Im Rahmen eines Workshops 1956 in Dartmouth wurde versucht, herauszufinden, wie man Maschinen dazu bringen kann, Sprache zu benutzen oder unterschiedliche Arten von Problemen zu lösen, die bisher dem Menschen vorbehalten waren.

Seit damals hat sich viel geändert und in der Zwischenzeit kommen KI-Lösungen in vielen Bereichen (und oft unerkannt) zum Einsatz (Sprach-, Muster- oder Gesichtserkennung, in der Cybersecurity, bei selbstfahrenden Fahrzeugen, ...). Neuen Aufwind hat die KI durch sogenannte generative KI und als bekanntestes Beispiel das Sprachmodell ChatGPT erhalten, das große Aufmerksamkeit erhielt, da es menschliche Sprache sehr eindrucksvoll nachahmte.

Da KI-Technologien in vielen wirtschaftlichen und privaten Bereichen Vorteile mit sich bringen, technische Innovationen jedoch auch immer mit Gefahren für den Menschen verbunden sein können, hat die EU am Abschluss einer rechtlichen Regelung gearbeitet, in der auch auf Gefahren der KI wie z. B. Diskriminierung oder Verletzung des Datenschutzes hingewiesen wurde.

Seit dem 1. August 2024 ist nun EU-weit und in Österreich die EU-Verordnung 2024/1689 zur Künstlichen Intelligenz (kurz KI-VO oder AI Act) in Kraft. Die konkreten Bestimmungen werden stufenweise in Geltung treten, wobei das Ziel der KI-VO ein sicherer und vertrauenswürdiger Einsatz von KI sowie die Schaffung eines einheitlichen und hohen Schutzniveaus ist.

Ein „KI-System" ist ein maschinengestütztes System, das

- für einen in unterschiedlichem Grad autonomen Betrieb ausgelegt ist,
- nach seiner Einführung anpassungsfähig sein kann und
- aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.

Die KI-VO verfolgt einen risikobasierten Ansatz und teilt KI-Systeme in verschiedene Risikostufen ein. Seit dem 2. Februar 2025 gelten Regelungen, die den Einsatz bestimmter KI-Systeme verbieten (Art 5 KI-VO). Besonders wichtig ist das Verbot von Emotionserkennungs- und biometrischen Kategorisierungssystemen am Arbeitsplatz. Emotionserkennungssysteme überwachen z. B. die Leistung und den emotionalen Zustand der Mitarbeiter:innen durch Analyse von Gesichtsausdrücken und Stimmton. Ab dem 2. August 2025 sind unter anderem die Bestimmungen zu KI-Modellen mit allgemeinem Verwendungszweck (General Purpose AI) verpflichtend anzuwenden und die Strafbestimmungen zu beachten (letztere gelten abweichend bei KI-Modellen mit allgemeinem Verwendungszweck erst mit 2.8.2026).

Im Anhang III der KI-VO werden KI-Systeme im Bereich Beschäftigung und Personalmanagement als Hochrisiko-KI-Systeme eingestuft (Art 6 Abs 2 KI-VO). Arbeitgeber:innen (als Betreiber:innen) müssen vor der Inbetriebnahme oder Verwendung eines Hochrisiko-KI-Systems am Arbeitsplatz die betroffenen Arbeitnehmer:innen und ihre Vertretungen informieren, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen werden. (Art 26 Abs 7 KI-VO). Betreiber von Hochrisiko-KI-Systemen haben eine Reihe von Pflichten, die vor allem in Art 26 der KI-VO geregelt sind und in Bezug auf Hochrisiko-KI-Systeme besteht außerdem das Recht auf menschliche Aufsicht. Diese Systeme müssen während ihrer Verwendung von natürlichen Personen effektiv überwacht werden (Art 14, 26 Abs 2 KI-VO).

Zudem muss im Unternehmen KI-Kompetenz aufgebaut werden (Art 4 KI-VO). Seit 2. Februar 2025 müssen Arbeitgeber:innen dafür sorgen, dass alle Mitarbei-

ter:innen, die mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über genügend KI-Kompetenz zur Anwendung der Systeme verfügen.

Hinzuweisen ist, dass die KI-VO die Geltung der nationalen Arbeitsrechtsvorschriften, somit die Arbeitnehmer:innenrechte und die Mitbestimmung durch die Interessenvertretung sowie die Regelungen zum Datenschutz, unberührt lässt (Art 3 Abs 11 KI-VO).

7.1 KI und das ArbVG

Die Einführung und der Einsatz Künstlicher Intelligenz am Arbeitsplatz führen sowohl zu Herausforderungen als auch zu Veränderungen und betreffen zweifellos die wirtschaftlichen und sozialen Interessen der Arbeitnehmer:innen. Eine rechtzeitige Einbindung und Mitbestimmung durch den Betriebsrat oder die Personalvertretung ist daher essenziell, um die Repräsentanz und Teilhabe der Arbeitnehmer:innen zu gewährleisten.

Grundlegend sind umfassende Informationspflichten der Arbeitgeberin bzw. des Arbeitgebers. Über den Auskunftsanspruch gemäß § 91 Abs 1 ArbVG erfährt der Betriebsrat, ob und in welchen Bereichen KI-Tools eingesetzt werden. Weil durch derartige Systeme idR auch personenbezogene Daten der Nutzer:innen, d. h. der Arbeitnehmer:innen, erfasst und verarbeitet werden, besteht zudem eine Mitteilungspflicht der Arbeitgeberin bzw. des Arbeitgebers gemäß § 91 Abs 2 ArbVG (von sich aus) über die „Arten" der personenbezogenen Arbeitnehmer:innendaten sowie darüber, welche Verarbeitungen und Übermittlungen vorgesehen sind. Auf Verlangen müssen dem Betriebsrat Unterlagen zur Verfügung gestellt werden, aus denen der Leistungsumfang des Systems ersichtlich ist. § 92a Abs 1 Satz 2 Z 1 ArbVG gewährt außerdem ein spezifisches Anhörungs- und Beratungsrecht bei der Einführung neuer Technologien, die die Arbeitsbedingungen beeinflussen. Der Betriebsrat ist bezüglich der Auswirkungen anzuhören, welche diese für die Sicherheit und Gesundheit der Arbeitnehmer:innen haben. In Bezug auf Hochrisiko-KI-Systeme hat der Betriebsrat zusätzlich das Recht, eine klare und umfassende Erklärung über die Rolle des Systems im Entscheidungsprozess sowie die wesentlichen Elemente der getroffenen Entscheidung zu erhalten (Art 86 KI-VO).

Relevanz haben weiters die Betriebsvereinbarungstatbestände, die dem Betriebsrat zur Verfügung stehen, um die näheren Bedingungen festzulegen, unter denen die Arbeitgeber:innen ein geplantes KI-Tool einsetzen dürfen. In vielen Fällen fallen KI-gesteuerte Systeme unter den Begriff der Kontrollmaßnahme oder des technischen Systems zur Kontrolle der Arbeitnehmer:innen, welche die Menschenwürde iSd § 96 Abs 1 Z 3 ArbVG berühren und damit die Zustimmungspflicht des Betriebsrates auslösen. Wenn die Menschenwürde nicht berührt wird, ist die Anwendbarkeit von § 96a ArbVG zu prüfen. Entscheidend ist hierbei, ob das System zur automationsunterstützten Erfassung und Datenverwendung von personenbezogenen Daten geeignet ist. In betriebsratslosen Betrieben ist die Einführung und der Einsatz von KI-Systemen nach entsprechender Zustimmung der Arbeitnehmer:innen möglich (§ 10 AVRAG).

Zu beachten ist, dass der Einsatz von KI-Tools auch eine Betriebsänderung darstellen kann, wenn er die Einführung neuer Arbeitsmethoden sowie Rationalisierungs- und Automatisierungsmaßnahmen von erheblicher Bedeutung zum Inhalt hat. Hierbei sind die Mitwirkung des Betriebsrates gemäß § 109 ArbVG und der Abschluss von Betriebsvereinbarungen/Sozialplänen nach § 97 Abs 1 Z 4 ArbVG zu beachten.

7.2 KI und ergänzende Regelungen durch die DSGVO

Auch die DSGVO enthält umfassende Informations- und Transparenzpflichten. Im Zusammenhang mit dem Einsatz von KI-Tools am Arbeitsplatz sei insbesondere Art 22 DSGVO hervorgehoben.

Algorithmisches Management ermöglicht auf Basis großer (personenbezogenen) Datenmengen oder der Zusammenführung von Daten eine umfassende Möglichkeit der Auswertung und Entscheidungsfindung. Der Einsatz von Algorithmen und Künstlicher Intelligenz kann somit zur Überwachung, Steuerung und Optimierung von Arbeitsprozessen und Mitarbeiter:innenleistungen eingesetzt werden. Dabei sieht Art 22 DSGV vor, dass betroffene Arbeitnehmer:innen das Recht haben, nicht einer ausschließlich automatisierten Entscheidung einschließlich Profiling unterworfen zu werden, und sie haben aussagekräftige Informationen

über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu erhalten.

SKRIPTEN ÜBERSICHT

VÖGB

WIRTSCHAFT

WI-1 Einführung in die Volkswirtschaftslehre und Wirtschaftswissenschaften

WI-2 Konjunktur

WI-3 Wachstum

WI-4 Einführung in die Betriebswirtschaftslehre

WI-5 Beschäftigung und Arbeitsmarkt

WI-6 Lohnpolitik und Einkommensverteilung

WI-9 Investition

WI-10 Internationaler Handel und Handelspolitik

WI-12 Steuerpolitik

WI-13 Bilanzanalyse

WI-14 Der Jahresabschluss

WI-16 Standort-, Technologie- und Industriepolitik

Die einzelnen Skripten werden laufend aktualisiert.

POLITIK UND ZEITGESCHICHTE

PZG-1A Sozialdemokratie und andere politische Strömungen der ArbeiterInnenbewegung bis 1945

PZG-1B Sozialdemokratie seit 1945

PZG-2 Christliche Soziallehre

PZG-4 Liberalismus/Neoliberalismus

PZG-6 Rechtsextremismus

PZG-7 Faschismus

PZG-8 Staat und Verfassung

PZG-9 Finanzmärkte

PZG-10 Politik, Ökonomie, Recht und Gewerkschaften

PZG-11 Gesellschaft, Staat und Verfassung im neuzeitlichen Europa, insbesondere am Beispiel Englands

PZG-12 Wege in den großen Krieg

PZG-14 Die Geschichte der Mitbestimmung in Österreich

SOZIALE KOMPETENZ

SK-1 Grundlagen der Kommunikation

SK-2 Frei reden

SK-3 NLP

SK-4 Konfliktmanagement

SK-5 Moderation

SK-6 Grundlagen der Beratung

SK-7 Teamarbeit

SK-8 Führen im Betriebsrat

SK-9 Verhandeln

SK-10 Politische Rhetorik

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen: www.voegb.at/skripten

Endnoten

[1] Siehe „Verarbeitung personenbezogener Beschäftigtendaten und Grenzen betrieblicher Mitbestimmung in einer digitalisierten Arbeitswelt" unter https://www.forba.at/wp-content/uploads/2021/06/Verarbeitung-persbez-Daten-und-MitbestimmungFORBA-Bericht2021_DigiFonds.pdf, (aufgerufen Juli 2025).

[2] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679, (aufgerufen Juli 2025).

[3] https://www.sicherheitshandbuch.gv.at/, (aufgerufen Juli 2025).

[4] Eine detaillierte Beschreibung der angeführten IT-Systeme findet sich in Haslinger S., Krisch A., Riesenecker-Caba Th. (Hrsg): Beschäftigtendatenschutz Handbuch für die betriebliche Praxis, ÖGB-Verlag (2020).

[5] https://dsb.gv.at/ueber-die-datenschutzbehoerde/newsletter, (aufgerufen Juli 2025).

[6] https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html, (aufgerufen Juli 2025).

Zum Autor

Mag.ª Martina Chlestil ist Juristin und arbeitet in der Arbeiterkammer Wien ua in den Themenbereichen Beschäftigtendatenschutz und Arbeitsverfassungsrecht.

Thomas Riesenecker-Caba, Studium der Betriebsinformatik, Geschäftsführer der Forschungs- und Beratungsstelle Arbeitswelt (FORBA) in Wien und dort für das Thema „Technikgestaltung und Datenschutz" verantwortlich. Er berät und schult Betriebsräte seit über 30 Jahren bei der Einführung, Gestaltung und Regelung von IKT-Systemen.
https://www.forba.at/forba_mitarbeiter/mag-thomas-riesenecker-caba/

Adriana Mandl ist Juristin mit Schwerpunkt auf Individual- und Kollektivarbeitsrecht in der Abteilung Sozialpolitik der Arbeiterkammer Wien.