Martina Chlestil, Thomas Riesenecker-Caba

Verarbeitung von personenbezogenen MitarbeiterInnen-Daten

Mitbestimmung und Datenschutz

5 Praktische Gewerkschaftsarbeit

Praktische Gewerkschaftsarbeit 5

Verarbeitung von personenbezogenen MitarbeiterInnen-Daten

Mitbestimmung und Datenschutz

Martina Chlestil
Thomas Riesenecker-Caba

Verarbeitung von personenbezogenen MitarbeiterInnen-Daten

Mitbestimmung und Datenschutz

ÖGB | AK ÖSTERREICH

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**

Stand: März 2022

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

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

Inhalt

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 zB Smartphones und nicht zuletzt die Verlagerung der eigentlichen Datenverarbeitung in die Cloud sind Zeichen dieses nachhaltigen betrieblichen Wandels. Parallel dazu vergrößerte sich jedoch auch die Gefahr von Angriffen auf die betriebliche IT über Netzwerke oder Geräte. Schadsoftware, Viren oder höchstprofessionelle Cyberangriffe erfordern umfassende Maßnahmen zum Datenschutz und der Systemsicherheit.

In diesem Umfeld versuchen betriebliche Interessenvertretungen wie Betriebsrat oder Personalvertretung die Verarbeitung von personenbezogenen Daten der MitarbeiterInnen 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 MitarbeiterInnen-Daten vermittelt
- zentrale Fragen zu Mitbestimmung und Datenschutz anschaulich erklärt und
- Hinweise zur betrieblichen Herangehensweise geliefert

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

2 Stand der Technik

Die Verarbeitung personenbezogener MitarbeiterInnendaten 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 mehr 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 des/der ArbeitgeberIn und den zur Verfügung gestellten Informationen ab.

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

- 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 (zB über Protokolle).

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.

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

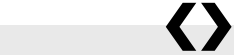
Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ([...] „betroffene Person") beziehen;

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 Daten 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 (zB 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 (zB Abholen eines Kopierauftrags, 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(n) personifizierten Chip(karte) oder ein nur ihr bekanntes Kennwort an einer Kopier-/Druckstation an, um einen Druckauftrag zu erhalten.
- Ein/e ArbeiterIn in einem Produktionsbetrieb meldet sich zu Schichtbeginn über Terminal an einer Maschine an und über Schicht-/ Dienstplan ist nachvollziehbar, wer diese Person ist.
- Ein/e FahrerIn ist mit einem Firmenfahrzeug unterwegs, das ihr/ihm zuvor zugeteilt wurde oder das sie/er über den Fahrzeugpool reserviert hat.

2 Stand der Technik

So können für unsere letzten beiden Beispiele erzeugte 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 Beispiel oder dessen Fahrzeugdaten, 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 (zB Maschinenbezeichnung, zugewiesener Arbeitsplatz im Call-Center),
- Standortdaten (zB GPS-Daten eines Fahrzeugs oder eines mobilen Endgeräts wie Smartphone oder Tablet, bei denen die GPS-Funktion eingeschaltet ist),
- eine Online-Kennung (zB IP-Adresse eines PCs: Die IP-Adresse ist für jedes Endgerät, das sich in einem Netzwerk anmeldet, eindeutig, 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) (zB Verknüpfung diverser Informationen im Rahmen einer Online-Befragung).

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

Überblick der personenbezogenen Daten

Eine der zentralen Grundsätze des Datenschutzrechts der bei der Verarbeitung von Daten zu berücksichtigen ist, ist die sogenannte Zweckbestimmung, dh 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) in einem System zu arbeiten, über die Erfassung gehaltsrelevanter Daten (zB Zeiterfassung, Bankverbindung), die Dokumentation der täglichen Arbeit (zB bearbeitete Belege) bis hin zur Sicherung des Unternehmens (zB Zutrittskontrolle, Videoerfassung).

Um hier nicht den Überblick zu verlieren, empfiehlt es sich, die im Unternehmen verarbeiteten personenbezogenen Daten nach verschiedenen Anwendungsbereichen zu unterscheiden. Diese Systematik (zB Einführung einer Datenklassifizierung) könnte auch eine 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 (zB wem darf welche Art von Information offengelegt werden oder was darf per E-Mail versendet werden).

2 Stand der Technik

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

- öffentlich
- intern
- vertraulich
- streng vertraulich

Abgeleitet von diesem Ansatz können personenbezogenen MitarbeiterInnendaten im Sinne der Bestimmungen des DSGVO/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
D	Geschäftsdaten	Diese Daten werden durch die Arbeit mit IT-Systemen erfasst und dokumentieren Tätigkeiten der ArbeitnehmerInnen. Beispiele: Bearbeitungsdauer (Beginn – Ende) eines Auftrages, Anzahl der täglichen Kontierungen

Klasse	Beschreibung	Erklärung/Beispiele
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, Fahrzeug)
G	Audio- und Videodaten	Audio- oder Bilddaten, die eindeutig einer Person zugewiesen werden können. Beispiele: Aufzeichnung Videomeeting, Bilder einer Überwachungskamera
H	Protokolldaten	Das Arbeiten in einem IT-System wird je 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
I	Inhaltsdaten	Daten/Informationen/Dokumente, die durch das individuelle Arbeiten der ArbeitnehmerInnen in den unterschiedlichen Services/Komponenten entstehen und personenbezogene Informationen enthalten können. Beispiele: Inhalt einer E-Mail oder eines Chats

2 Stand der Technik

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 Erkennbarkeit einer bestimmten Person (zB über deren Personalnummer) dieses Datum pseudonymisiert wird, dh durch einen nur der durchführenden Person (bzw einem äußerst kleinen Kreis) bekannten Code (zB 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 (zB verschlüsselten) Tabelle zu hinterlegen.

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."

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-6**	Grundlagen der Beratung
SK-2	Frei reden	**SK-7**	Teamarbeit
SK-3	NLP	**SK-8**	Führen im Betriebsrat
SK-4	Konfliktmanagement	**SK-9**	Verhandeln
SK-5	Moderation	**SK-10**	Politische Rhetorik

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

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 MitarbeiterInnendaten für unterschiedliches Zwecke verarbeitet werden.

In der Vergangenheit waren es vor allem Anwendungsgebiete wie Personalverrechnung, Zeiterfassung, Zutritts- oder Videokontrolle bzw. branchenspezifische Anwendungsbereich wie Call-Center-Steuerung oder Produktionsplanung. Durch die Vernetzung von Geräten (zB Smartphones) und den globalen Datenaustausch zwischen Betrieben (zB 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 der verschiedenen Einsatzgebiete[4] und mögliche (datenschutzrechtliche) Verwendungszwecke. Inwieweit diese IT-Systeme im jeweils eigenen Unternehmen zum Einsatz kommen, ist einerseits vom/von der ArbeitergeberIn 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, Personalentwicklung (MitarbeiterInnen-Gespräche, Skills), e-Learning , digitaler Personalakt, HR Cloud (SAP SuccessFactors, Workday)
Betriebliche Verwaltungssysteme, ERP-Enterprise Resource Planning-Systeme	Buchhaltung, Controlling, Lagerverwaltung, Einkauf, Vertrieb, ...

Einsatzgebiete	Verwendungszwecke
Kommunikationssysteme	Telefon, mobile Kommunikation (Smartphones inkl. Apps), E-Mail, Internet, Intranet
Kollaborationssysteme	Videokonferenzen (zB Teams, Zoom), Verwendung sozialer Medien (Workplace von Facebook, Microsoft Yammer, SAP JAM), Messenger-Dienste (WhatsApp, Signal, ...)
Verwaltungssoftware	MDM (Mobile Device Management), Multifunktionsgeräte, HelpDesk, BenutzerInnenverwaltung (AD = Active Directory)
Kontrollsysteme	Zutrittskontrolle, Videoüberwachung
Cloud Anwendungen	Microsoft 365 (Office 365, EMS = Enterprise Mobility + Security, Windows Enterprise, Dynamics 365)
Branchenspezifische Lösungen	IT-Systeme in der Produktion (Betriebsdatenerfassung, Produktionsplanung und -steuerung), Call Center, Fuhrpark-/Fahrzeugverwaltung (Flottenmanagement, GPS, Fahrzeugborddaten), Tätigkeitserfassung, Qualitätssicherung (zB Mystery Calls), Ausgabeautomaten
IT-Sicherheit	Firewall, SIEM (Security Information and Event Management), UBA/UEBA (User and Entity Behavior Analytics), ISMS (Information Security Management System), Security Training (Phising)
Datenbank-Lösungen/ künstliche Intelligenz (KI)	Business Intelligence, Data Warehouse, Big Data, SAP HANA, Künstliche Intelligenz (Mustererkennung, Automatisierung betrieblicher Prozesse)
Hinweisgebersystem (Whistleblowing)	Einbringen (anonymer) Hinweise, Einhaltung betrieblicher Compliance-Regelungen

3 Technische Systeme

Einsatzgebiete	Verwendungszwecke
online-Befragungstools	MitarbeiterInnen-Befragungen, Stimmungsanalysen
MitarbeiterIn in anderer Rolle	MitarbeiterIn als KundIn im betriebsinternen CRM-System oder in der KundInnen-/KlientInnenverwaltung, vor Eintritt in das Unternehmen Datenverarbeitung als BewerberIn (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.

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

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 Arbeitnehmerinnen und Arbeitnehmer bei der Verarbeitung ihrer Daten im Betrieb zu wahren.

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 des/der ArbeitnehmerIn durch die DSGVO und das DSG eine zusätzliche Beschränkung des/der ArbeitgeberIn im Umgang mit Beschäftigtendaten durch kollektive Befugnisse.

Siehe dazu 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.

Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG

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

Überwachungsbefugnisse

Durch die in **§ 89 Satz 1 ArbVG** enthaltene Generalklausel ist ein umfassendes Überwachungsrecht des Betriebsrates bezüglich der Einhaltung aller die ArbeitnehmerInnen berührenden Normen (zB 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 BetriebsinhaberIn ergeben.

Neben der umfassenden Umschreibung des Überwachungsrechts des Betriebsrates mittels einer Generalklausel werden einzelne Überwachungsbefugnisse durch die beispielsweise Aufzählung (§ 89 Z 1 bis 4 ArbVG) ausgeformt. Nach § 89 Z 1 ArbVG hat der Betriebsrat das Recht, in die vom/von der ArbeitgeberIn geführten Aufzeichnungen über die Bezüge der ArbeitnehmerInnen und die zur Berechnung dieser Bezüge erforderlichen Unterlagen Einsicht zu nehmen und insbesondere auf ihre Richtigkeit zu überprüfen. Das Recht auf Einsichtnahme in die Gehaltsunterlagen wird auch auf andere die ArbeitnehmerInnen 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 erhält das Überwachungsrecht des Betriebsrates insofern, als dem Betriebsrat die Informationen in einem Ausmaß

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

Hinzuweisen ist auf die strenge Verschwiegenheitsplicht nach § 115 ArbVG, der der Betriebsrat und dessen Mitglieder unterliegen. Eine Weitergabe oder Veröffentlichung von Daten einzelner ArbeitnehmerInnen 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 den/die ArbeitgeberIn zu überprüfen. Die dazu erforderlichen Informationen hat der/die ArbeitgeberIn durch Einsicht in die dazu nötigen Unterlagen zu gewähren.

Informationsrechte

Auskunftspflicht des/der ArbeitgeberIn nach § 91 Abs 1 ArbVG

Gemäß § 91 Abs 1 ArbVG ist der/die BetriebsinhaberIn verpflichtet, dem Betriebsrat auf Anfrage über alle Angelegenheiten, welche die wirtschaftlichen, sozialen, gesundheitlichen oder kulturellen Interessen der ArbeitnehmerInnen des Betriebes berühren, Auskunft zu erteilen.

Der Gesetzgeber hat erkannt, wie bedeutend die Information für eine effektive Interessenvertretung der Arbeitnehmerschaft 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 ArbeitgeberInnen nicht aus Überraschungseffekten, Zeitnot, Desorientierung der ArbeitnehmerInnen oder auch „vollendeten Tatsachen" Vorteile ziehen können. Die Information muss die Thematik vollständig 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, ArbeitnehmerInneninteressen betreffendes Auskunftsrecht des Betriebsrates besteht: Die Angelegenheit muss geeignet sein, Auswirkungen auf die oa Interessen der ArbeitnehmerInnen zu haben, es muss eine ausreichende und aktuelle Beziehung zu den ArbeitnehmerInneninteressen gegeben sein. Die Auskunftspflicht des Arbeitgebers des § 91 Abs 1 ArbVG entsteht bei entsprechend konkreten Verlangen des Betriebsrates (dies ist am besten nachweislich schriftlich zu übermitteln). Die Konkretheit der Anfrage beeinflusst die Informationspflicht des/der ArbeitgeberIn: Je mehr die Anfrage spezifiziert ist, desto genauer muss die Information sein. Der Betriebsrat kann, wenn der/die ArbeitgeberIn trotz konkreter Nachfrage hiezu 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 Mitarbeiterbefragungen kommen in Betrieben immer wieder vor. Anhand der mittels dem allgemeinen Auskunftsrecht gewonnen 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) des/der ArbeitgeberIn vorliegt bzw ob nicht doch personenbezogene Daten aufgenommen werden.

Informationspflicht des/der ArbeitgeberIn nach § 91 Abs 2 ArbVG

Ein echtes Informationsrecht des Betriebsrates besteht bei der Verarbeitung von personenbezogenen Beschäftigtendaten: Gemäß § 91 Abs 2 ArbVG haben ArbeitgeberInnen dem Betriebsrat von sich aus Mitteilung zu machen, welche Arten von personenbezogenen ArbeitnehmerInnendaten 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 des/der ArbeitgeberIn (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 ArbeitnehmerInnen hat der Betriebsrat, sofern dies nach § 89 ArbVG oder anderen Rechtsvorschriften erlaubt ist oder der/die betroffene ArbeitnehmerIn 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 ArbeitnehmerInnen Einsicht zu nehmen. Ebenso wird keine Zustimmung einzelner ArbeitnehmerInnen erforder-

lich 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 ArbeitnehmerInnen 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.

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 personenbezogen Daten von ArbeitnehmerInnen 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 des/der ArbeitgeberIn zu blockieren oder gar zu verhindern, sondern der Belegschaft (vertreten durch den Betriebsrat) eine starke Verhandlungsposi-

tion 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 vom/von der ArbeitgeberIn rechtzeitig (dh bereits in der Planungsphase) zu informieren und miteinzubeziehen, sodass er die berechtigten ArbeitnehmerInneninteressen noch einbringen kann. In der Betriebsvereinbarung sind die näheren Bedingungen festzulegen, unter denen der/die ArbeitgeberIn 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. Dh, selbst wenn sich ein System bereits seit geraumer Zeit in Betrieb befindet, ist – bei Vorliegen der Voraussetzungen – eine Betriebsvereinbarung dazu abzuschließen. Ebenso müssen ArbeitgeberInnen neu mit dem Betriebsrat verhandeln, wenn das System entsprechende 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 27.05.2004, 8 ObA 97/03b).

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

Betriebsvereinbarungen nach § 96 ArbVG

Bei den Tatbeständen des § 96 ArbVG handelt es sich um Fälle der **notwendigen Mitbestimmung** – dh 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 des/der ArbeitnehmerIn 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 des/der ArbeitnehmerIn 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 des/der BetriebsinhaberIn zustimmungspflichtig sein, die geeignet sind, dem/der ArbeitgeberIn Informationen über persönliche Umstände oder Meinungen eines/einer einzelnen ArbeitnehmerIn zu verschaffen, an deren Geheimhaltung diese/r ein Interesse haben könnte; anonymisierte MitarbeiterInnenbefragungen seien auch ohne Zustimmung des Betriebsrates zulässig: Entscheidend für die Zustimmungspflicht ist, ob die Aktion so angelegt ist, dass der/die ArbeitgeberIn durch sie in den Besitz personenbezogener Daten und Informationen gelangen kann. Nicht von Bedeutung ist, ob die Fragebogenaktion von ihm/ihr 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 der/die ArbeitgeberIn keine personenbezogenen Informationen erhält bzw die Informationen keine Rückschlüsse auf bestimmte ArbeitnehmerInnen ermöglichen und der/die BetriebsinhaberIn 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 (zB 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 ArbeitnehmerInnen 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 ArbeitnehmerInnen 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 Entfal-

tung der Persönlichkeit des/der ArbeitnehmerIn 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 des/der ArbeitgeberIn für den Einsatz einer Kontrollmaßnahme besteht (zB Schutz der Sicherheit und Gesundheit von Personen, Schutz des Eigentums des/der ArbeitgeberIn), hat der Betriebsrat im Rahmen des Abschlusses der Betriebsvereinbarung zu berücksichtigen und auch die nötigen Schutzmaßnahmen für die ArbeitnehmerInnen vor unverhältnismäßiger Überwachung vorzusehen.

In betriebsratslosen Betrieben dürfen solche Kontrollmaßnahmen nur mit Zustimmung der einzelnen ArbeitnehmerInnen durchgeführt werden, die jederzeit widerrufen werden kann, sofern keine schriftliche Vereinbarung über ihre Dauer getroffen wurde.

Maßnahmen, die die Menschenwürde verletzen, sind – selbst mit Zustimmung des Betriebsrates bzw des/der ArbeitnehmerIn – 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 TeilnehmerInnen 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).

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 ArbeitnehmerInnen, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen, der Abschluss einer Betriebsvereinbarung erforderlich. Eine Zustimmung ist nicht erforderlich, 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 (zB Name, Familienstand, Geburtsdatum) und fachlichen Voraussetzungen (zB Ausbildungsweg, Schulabschluss, besondere berufliche Qualifikationen, die zuletzt ausgeübte

Tätigkeit etc) hinausgehen. Dabei ist zu beachten, dass zustimmungsfrei nur die Ermittlung dieser so genannten „schlichten ArbeitnehmerInnendaten" ist. Werden ArbeitnehmerInnendaten dieser Art in weiterer Folge automationsunterstützt verarbeitet, also insbesondere miteinander oder mit anderen Datenbeständen verknüpft, oder übermittelt (dh an andere EmpfängerInnen 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 des/der ArbeitgeberIn in einer einschlägigen Rechtsquelle vorgesehen sein, bestimmte Daten in bestimmter Weise zu verwenden. Als Beispiele dafür wären die An- und Abmeldung von ArbeitnehmerInnen 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, 8ObA 97/03b).

Beispiele:

In der Praxis kommen in den allermeisten Fällen Personalinformationssysteme zur Anwendung, mit Hilfe derer eine Fülle von Beschäftigtendaten zum Zweck der Personalverwaltung und der rascheren und umfassenderen Personaldisposition miteinander verbunden und ausgewertet werden können (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 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 des/der ArbeitnehmerIn 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 ArbeitnehmerInnen 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.

Zweck des Mitwirkungsrechtes des Betriebsrates ist somit vor allem, durch die Einbringung der (individuellen und kollektiven) ArbeitnehmerInneninteressen zur Objektivierung des Beurteilungssystems und -verfahrens beizutragen. Eine Betriebsvereinbarung soll die Transparenz von Beurteilungssystemen für ArbeitnehmerInnen 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 in Frage kommen: So können Personalbeurteilungen uU 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 des/der ArbeitnehmerIn 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 des/der ArbeitgeberIn 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 Bewertungsverfahren 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 uU 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 „Whistle-Blowing"-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 der/die ArbeitgeberIn 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 dem/der ArbeitgeberIn 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.

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:

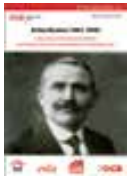
- Seminare
- ReferentInnen
- Alle, die an gewerkschaftlichen Themen interessiert sind.

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



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 bedürfte 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).

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 sind. *(Art 4 Z 6 DSGVO)*

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

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 nichtautomatisierte 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 einem Verantwortlichen vorgenommen wird, der 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 Datenschutzrecht

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 den Betroffenen 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 der Verantwortliche die Einhaltung der Grundsätze nachweisen muss. *(Art 5 Abs 2 DSGVO)*

Rechtmäßigkeit der Datenverarbeitung

Jede Verarbeitung personenbezogener Daten muss rechtmäßig sein. Das heißt, bei jeder Datenverarbeitung muss sich 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** 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)*

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 Kopie der Daten, die Gegenstand der Verarbeitung sind, ist vom 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 Vergessen**). *(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 einem anderen Anbieter 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 öffentlichem 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 und Verantwortliche zu datenschutzfreundlichen Produkten (Prozessen) und Voreinstellungen verpflichtet sind (**Privacy by Design/Privacy by Default**). *(Art 25 DSGVO)*

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 des Verantwortlichen
- Name und Kontaktdaten des Datenschutzbeauftragten (sofern bestellt)
- Zweck(e) der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern
- gegebenenfalls Übermittlungen von personenbezogenen 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 MitarbeiterInnen beschäftigen. Unternehmen und Einrichtungen, die weniger als 250 MitarbeiterInnen 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 ist 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 (zB 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 dazu können auf der Homepage der Datenschutzbehörde abgerufen werden (https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich). *(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.

Der/die 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 einen Datenschutzbeauftragten zu benennen.

Der Datenschutzbeauftrage benötigt eine entsprechende Qualifikation und Fachwissen, er ist in seiner Funktion weisungsfrei, darf wegen seiner Tätigkeit nicht abberufen oder benachteiligt werden und unterliegt einer Verschwiegenheitspflicht. *(Art 37, Art 38 DSGVO)*

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

- die Betroffenen zu unterrichten und ihnen Auskunft zu erteilen
- das Einhalten des Datenschutzrechts zu überwachen (zB die Abhaltung von Schulungen für MitarbeiterInnen)
- die Verantwortlichen (die Unternehmensführung) zu unterstützen
- der höchsten Managementebene zu berichten
- mit der Behörde zusammenzuarbeiten, insbesondere iZm der Datenschutz-Folgenabschätzung *(Art 39 DSGVO)*

5 Datenschutzrecht

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 Einschau in Datenverarbeitungen und Unterlagen, bei der der Verantwortliche bzw Auftragsverarbeiter zur Mitwirkung und Unterstützung verpflichtet ist und sogenannte Abhilfebefugnisse. Damit kann die Behörde rechtwidriges 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)*

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 der Kläger 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 (zB bei einem Verstoß gegen die Bestimmungen über die Füh-

rung 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 (zB 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 ua 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 (zB 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)*

Betriebsrat 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.

Hinzuweisen ist, dass generell die Vorschriften der DSGVO und des DSG (zB die allgemeinen Grundsätze der Datenverarbeitung, die Zulässigkeit einer konkreten Datenverwendung, die Rechte der betroffenen Personen, weitere datenschutzrechtlichen Verpflichtungen 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 des/der ArbeitnehmerIn bindet.

Frageliste zu IT-Systemen

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

Der/die ArbeitgeberIn ist, wie oben im Kapitel 4 „Arbeitsverfassung" zu den Informationspflichten nach § 91 Abs 2 ausgeführt, zur umfassenden Beantwortung dieser Fragen verpflichtet. 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 Cloudanwendung?
- Für welche(n) Verarbeitungszweck(e) 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 auch eigene Auswertungen flexibel gestalten?
- Sind Datenübermittlungen vom IT-System zu anderen IT-Systemen geplant (Beschreibung der technischen Schnittstellten oder Downloadmöglichkeit zB in Excel)?

- Werden personenbezogene Daten an Dritte (andere Konzernteile, Auftragsverarbeiter, ...) 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 ergrifefn?

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

„Spielregeln" für die Verarbeitung personenbezogener MitarbeiterInnendaten – die Rahmen-Betriebsvereinbarung

Die umfassenden neuen Anforderungen, die die DSGVO mit sich bringt 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 Länder, die eine ähnliche Form der Mitwirkung und -gestaltung des Betriebsrates in ihrem Arbeitsrecht kennen, der Abschluss 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 ArbeitgeberIn und Betriebsrat unabhängig vom eingesetzten System geregelt werden können, quasi als Spielregel für die Regelung der unterschiedlichen Systeme.

Bei der Durchsicht bisher abgeschlossener Betriebsvereinbarungen zu einzelnen Systemen zeigt sich, dass diese Vereinbarungen zwei große Regelungsbereiche

aufweisen: Zum einen werden technische Aspekte zum konkreten System geregelt, wie zB 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 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, zB in welcher Form der Betriebsrat informiert und in Änderungsprozesse einbezogen wird, welche Rechte und Pflichten die Beschäftigten besitzen, deren Daten verarbeitet werden und wie AuftragsverarbeiterInnen 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 ArbeitgeberIn 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 die einzelnen Systeme sind dann die jeweils spezifischen technischen Details als Zusatz-Betriebsvereinbarung auszuhandeln.

Betriebsvereinbarungen für konkrete IT-Systeme

Für konkrete IT-Systeme, die personenbezogene MitarbeiterInnendaten verarbeiten, kann nach Abschluss der Rahmen-Betriebsvereinbarung unterschiedlich 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, zB mit Kontrollmaßnahmen, der Abschluss einer (Zusatz)Betriebsvereinbarung notwendig sein. Als Zwischenlösung könnte auch ein Datenblatt mit der Beschreibung des IST-Standes, dh 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
- Rollen- und Berechtigungskonzept
- (optional) organisatorische Regeln (technische organisatorische Maßnahmen TOMs)

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.

Fußnoten

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

2 https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679

3 https://www.sicherheitshandbuch.gv.at/

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://www.dsb.gv.at/download-links/newsletter.html (aufgerufen Februar 2021)

AutorInnen

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/