

Hinweis zur folgenden Checkliste

Anhand der folgenden Fragen kann seitens des Betriebsrates erhoben werden, welche Informations- und Kommunikationssysteme im eigenen Unternehmen im Einsatz sind bzw. welche Verarbeitungen geplant sind.

Diese Information liefert somit die Grundlage, in welchen Bereichen die Verarbeitung personenbezogener Daten im Hinblick auf die datenschutzrechtlichen Bestimmungen (DSGVO und DSG) und arbeitsrechtlichen Bestimmungen (Mitwirkungsrechte des Betriebsrates nach ArbVG) zwischen Unternehmen und Betriebsrat zu regeln ist.

Weitere Informationen finden sich unter <https://www.forba.at/beratung/>

Die rechtlichen Bestimmungen zum Datenschutz finden sich unter anderem auf der Webseite der *Österreichischen Datenschutzbehörde*

<https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html>

Erklärungen zu den rechtlichen Bestimmungen finden sich zudem in der VÖGB-Broschüre „*Verarbeitung von personenbezogenen MitarbeiterInnen-Daten*“ (Stand März 2022) der Autor:innen Martina Chlestil (AK Wien) und Thomas Riesenecker-Caba (FORBA).

Freier Download unter: <https://www.voegb.at/skripten-und-broschueren/praktische-gewerkschaftsarbeit/verarbeitung-von-personenbezogenen-mitarbeiterinnen-daten>

Das folgende Dokument kann durch den Betriebsrat unter Setzung einer Frist zur Beauskunftung übernommen und an die betriebliche Praxis angepasst werden.

Information des Betriebsrates nach § 91 ArbVG

Neben den Mitbestimmungsrechten der Arbeitsverfassung beeinflusst auch die EU-Datenschutz-Grundverordnung (DSGVO) die Verarbeitung personenbezogener Daten der Beschäftigten im Betrieb und Konzern.

Für alle Verarbeitungstätigkeiten in sämtlichen (Datei-)Systemen muss – wie in Folge noch näher beschrieben wird – nicht nur Rechenschaft über die **Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten** (nach Artikel 5 DSGVO) gelegt werden, sondern darüber hinaus ein **Verzeichnis aller Verarbeitungstätigkeiten** (nach Artikel 30 DSGVO) geführt werden.

Darüber hinaus können die Mitgliedstaaten nach Artikel 88 DSGVO „*durch Rechtsvorschriften oder durch Kollektivvereinbarungen* (nach Erwägungsgrund 155 einschließlich Betriebsvereinbarungen) *spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext ... vorsehen*“. Österreich hat dazu keine neuen Bestimmungen erlassen, weist jedoch auf die Bedeutung des Arbeitsverfassungsgesetzes hin (vgl. Mitteilung der Republik Österreich zu Art. 88 Abs. 3 Datenschutz-Grundverordnung: [Verordnung EU Nr. 2016/679] siehe dazu:

https://commission.europa.eu/system/files/2019-02/at_notification_art_88.3_complement_publish.pdf

Um diesen Anforderungen zu genügen und in Verbindung mit den Bestimmungen des Arbeitsverfassungsgesetzes rechtskonform zu agieren, ersucht der Betriebsrat binnen **x Tagen/Wochen** um schriftliche Beantwortung der folgenden Fragen:

- 1. Welche Informations- und Kommunikationssysteme (IKT-Systeme) im Unternehmen verarbeiten personenbezogene Beschäftigtendaten?**

Rechtlicher Hintergrund

Nach **§ 91 Abs 2 ArbVG** hat der Betriebsinhaber

„dem Betriebsrat Mitteilung zu machen, welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht.“

Als personenbezogene Daten definiert **Artikel 4 DSGVO**

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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.“

Diese weite rechtliche Begriffsdefinition bedeutet, dass nicht unbedingt ein direkter Personenbezug über Personalnummer oder Name vorliegen muss, sondern der Personenbezug auch aus der Verknüpfung mehrerer Daten abgeleitet werden könnte (beispielsweise Stückzahlen einer Produktionsmaschine in Verbindung mit der Zuteilung einer Person zu dieser Maschine).

Erwartete Antwort:

Auflistung aller IKT-Systeme, die personenbezogene Daten von Beschäftigten verarbeiten. Zusätzlich sind je System folgende Angaben beizufügen bzw der Auszug aus dem Verzeichnis von Verarbeitungstätigkeiten (siehe Art. 30 DSGVO) beizulegen:

- Übersicht der verwendeten Datenarten inkl. geplante Speicherdauer
- Verwendungszwecke (Grund der Verarbeitung, geplante personenbezogene Auswertungen/Analysen/Kennzahlen)
- Übersicht technischer Schnittstellen zu anderen Systemen (d.h. an welche anderen Systeme werden welche personenbezogenen Daten übermittelt)
- Information, ob personenbezogene Daten an Dritte (andere Konzernteile, Auftragsverarbeiter, ...) übermittelt werden und auf Basis welcher Rechtsgrundlage dieser Datentransfer beruht (dies könnte der Fall sein, wenn Daten österreichischer Beschäftigter durch einen Dritten verarbeitet werden, beispielsweise zur Personalverrechnung oder zur Personalverwaltung im Konzern)
- Berechtigungskonzept (Rollenbeschreibung), d.h. wer hat Zugriff auf die Daten
- getroffene Datensicherheitsmaßnahmen nach **Artikel 24 und 32 DSGVO**

Der Großteil dieser Informationen findet sich im Verzeichnis aller Verarbeitungstätigkeiten nach **Artikel 30 DSGVO**, das in jedem Unternehmen seit 25. Mai 2018 geführt werden muss.

In diesem Zusammenhang ist für jedes IKT-System zu prüfen, inwieweit die Grundsätze für die Verarbeitung personenbezogener Daten nach Artikel 5 DSGVO eingehalten werden.

Artikel 5 DSGVO regelt die Grundsätze für eine rechtskonforme Verarbeitung personenbezogener Daten wie folgt:

(1) *Personenbezogene Daten müssen*

a) *auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);*

b) *für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; (...)* („**Zweckbindung**“);

c) *dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);*

d) *sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“);*

e) *in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; (...)* („**Speicherbegrenzung**“);

f) *in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“);*

(2) *Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („**Rechenschaftspflicht**“).*

Sofern ein System von einem Auftragsverarbeiter betrieben wird und diesem Beschäftigtendaten zur Verfügung gestellt werden, ist der Name des Auftragsverarbeiters anzuführen und darauf hinzuweisen, wann die Vereinbarung zur Auftragsdatenverarbeitung abgeschlossen wurde und wo diese betriebsintern eingesehen werden kann. Dies trifft auch auf Verarbeitungen von Beschäftigtendaten zu, die in anderen Konzerntöchtern bzw. bei der Konzernmutter stattfinden!

Anforderungen an die Vertragsgestaltung mit einem Auftragsverarbeiter finden sich in den **Artikeln 28 und 29 DSGVO**.

2. Welche Unterlagen gibt es zu den unter Punkt 1 angeführten Informations- und Kommunikationssystemen?

Aus diesen Unterlagen (z.B. Systembeschreibung, Anwenderhandbuch) sollte der Leistungsumfang der Systeme ersichtlich sein, um abschätzen zu können, ob für die verschiedenen IKT-Systeme im Hinblick auf die Verarbeitung von personenbezogenen Beschäftigtendaten der Abschluss einer Betriebsvereinbarung nach § 96 bzw. 96a ArbVG notwendig ist. Diese Unterlagen können in elektronischer Form oder auf Papier zur Verfügung gestellt werden.

Rechtlicher Hintergrund

Nach **§ 91 Abs 2 ArbVG** ist dem Betriebsrat

„auf Verlangen die Überprüfung der Grundlagen für die Verarbeitung und Übermittlung zu ermöglichen.“

Nach **§ 96a Abs 1 ArbVG** bedürfen folgende Maßnahmen des Betriebsinhabers zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates:

„1. Die Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen. 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“

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 offen zu legen sind (siehe OGH-Entscheidung 8ObA97/03b).

Nach **§ 96 Abs 1 ArbVG** bedürfen folgende Maßnahmen des Betriebsinhabers zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates:

„3. die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren“

Auch die Kontrolle rein dienstlichen Verhaltens kann zustimmungspflichtig sein. Vor allem durch zu große, über das für die Erreichung des Kontrollzwecks erforderliche Ausmaß hinausgehende Kontrolldichte bei der Arbeit kann die Menschenwürde iSd § 96 Abs 1 Z 3 ArbVG tangiert werden. Es kommt also auf die Intensität der Kontrolle an. 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 (siehe OGH-Entscheidung 9ObA109/06d).

Erwartete Antwort:

Auflistung aller im Unternehmen vorhandener Unterlagen zu den verwendeten IKT-Systemen und Nennung einer verantwortlichen (internen oder externen) Ansprechperson.

Aus der Analyse der Systembeschreibungen sollte nachvollziehbar sein, ob die zur Verfügung stehende Funktionalität über die Erfüllung von Verpflichtungen hinausgeht, *die sich aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag ergeben.*

3. Welche Veränderungen in der betrieblichen IKT-Landschaft sind in nächster Zeit im Hinblick auf die Verarbeitung personenbezogener Beschäftigtendaten geplant?

Die betriebliche IKT-Landschaft unterliegt einer schnellen Veränderung. Systemänderungen bzw. der Wechsel auf neue technische Lösungen treten in immer kürzeren Zeitabständen auf. Ist eine Systemänderung bzw. die Einführung eines neuen IKT-Systems mit der Verarbeitung personenbezogener Mitarbeiterdaten verbunden, hat der Betriebsinhaber neben der Erfüllung der datenschutzrechtlichen Anforderungen auch den Betriebsrat rechtzeitig einzubinden.

Rechtlicher Hintergrund

Nach **§ 91 Abs 2 ArbVG** hat der Betriebsinhaber

*„dem Betriebsrat Mitteilung zu machen, welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er **vorsieht**“.*

Darüber hinaus ist der Betriebsinhaber nach **§ 92a Abs 1 ArbVG** insbesondere verpflichtet

„1. den Betriebsrat bei der Planung und Einführung neuer Technologien zu den Auswirkungen zu hören, die die Auswahl der Arbeitsmittel oder Arbeitsstoffe, die Gestaltung der Arbeitsbedingungen und die Einwirkung der Umwelt auf den Arbeitsplatz für die Sicherheit und Gesundheit der Arbeitnehmer haben“

Weiters ist vom Betriebsinhaber, in seiner Rolle als datenschutzrechtlicher Verantwortlicher nach **Artikel 35 DSGVO** zu prüfen, ob für ein IKT-System vor Einführung eine *Datenschutz-*

Folgenabschätzung durchzuführen ist.

*„Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche **vorab** eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“*

In diesem Zusammenhang sei darauf hingewiesen, dass nach **Artikel 35 Abs 9 DSGVO** eine Beiziehung des Betriebsrates (als Vertreter der Beschäftigten) notwendig sein kann.

„Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.“

Erwartete Antwort:

Auflistung der im Unternehmen geplanten Änderungen im Zusammenhang mit der Verarbeitung personenbezogener Daten der Beschäftigten und Übermittlung der Dokumentation der Risikoabschätzung hinsichtlich der Notwendigkeit einer Datenschutz-Folgenabschätzung.

(Stand 2023)