

IT-SECURITY

Mitarbeiterdaten in KI-Tools: Betriebsrat-Pflichten Österreich

Wann braucht es eine Betriebsvereinbarung für KI-Tools? ArbVG, DSGVO und Haftung für österreichische KMU erklärt.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

2. August 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/mitarbeiterdaten-ki-tool-betriebsrat-pflichten-oesterreich/>

Ein Vertriebsmitarbeiter kopiert eine Kundenliste in ChatGPT, um eine Angebotsvorlage zu erstellen. Klingt nach einer harmlosen Produktivitätsmaßnahme — ist aber potenziell ein DSGVO-Verstoß, für den das Unternehmen haftet. Kommt dabei noch heraus, dass das Tool Leistungsdaten auswertet, wird auch das Arbeitsverfassungsgesetz relevant.

KI-Tools sind in österreichischen KMU längst Alltag. Die rechtlichen Spielregeln, die damit einhergehen, kennen die wenigsten Verantwortlichen. Wann muss der Betriebsrat zustimmen? Wann reicht eine Information? Und was passiert, wenn gar nichts geregelt ist?

Dieser Artikel beantwortet genau diese Fragen — mit konkreten österreichischen Szenarien, einer klaren Abgrenzung nach Datenkategorien und einem Schritt-für-Schritt-Prozess für die Betriebsvereinbarung. Er ersetzt keine Rechtsberatung, gibt aber die richtigen Leitfragen vor, bevor Sie mit Anwalt oder Betriebsrat in die Verhandlung gehen.

Warum KI-Tools eine neue Kategorie im Arbeitsrecht sind

Klassische Software macht, was man ihr sagt — und gibt dabei keine Daten weiter. KI-Tools funktionieren anders: Sie verarbeiten eingegebene Inhalte, speichern sie potenziell zur Modelloptimierung und können aus Eingaben von heute das Verhalten von morgen beeinflussen. Das macht sie zu einer eigenen rechtlichen Kategorie, auch wenn viele Unternehmen sie noch wie gewöhnliche Textprogramme behandeln.

Das österreichische Arbeitsverfassungsgesetz (ArbVG) kennt zwei zentrale Eingriffsstufen: die zustimmungspflichtige Maßnahme (§ 96 ArbVG) und die beratungspflichtige Maßnahme (§ 97 ArbVG). Welche Stufe greift, hängt davon ab, ob ein Tool zur Kontrolle von Mitarbeitern geeignet ist — nicht nur ob es dafür eingesetzt wird.

Die entscheidende Abgrenzungsfrage lautet: Kann dieses Tool Daten über das Verhalten, die Leistung oder die Anwesenheit von Mitarbeitern erfassen, auswerten oder aggregieren? Wenn ja, ist es ein „kontrollierendes“ System im Sinne des ArbVG — unabhängig davon, ob das der Einführungszweck war. Viele Unternehmen setzen solche Tools ein, ohne zu wissen, dass sie damit mitbestimmungspflichtige Systeme einführen.

§ 96 ArbVG – wann braucht es zwingend eine Betriebsvereinbarung?

§ 96 ArbVG regelt die zustimmungspflichtigen Maßnahmen. Darunter fällt die Einführung von Kontrollmaßnahmen und Kontrollsystemen, die die Menschenwürde berühren — eine Formulierung, die in der Praxis weit ausgelegt wird.

Konkrete Beispiele im KI-Kontext: – Ein KI-Tool trackt, wann Mitarbeiter am Computer aktiv sind (Anwesenheitskontrolle) – Ein Tool wertet Verkaufsgespräche oder E-Mail-Response-Zeiten automatisch aus (Leistungsmessung) – Eine KI analysiert Kommunikationsverläufe auf Stimmung oder Produktivitätsmuster

In allen drei Fällen ist eine Betriebsvereinbarung nicht optional, sondern Voraussetzung. Wird die Maßnahme ohne Zustimmung des Betriebsrats eingeführt, ist sie rechtsunwirksam. Der Betriebsrat kann auf Unterlassung klagen.

§ 97 ArbVG – Beratungsrecht vs. Zustimmungspflicht

Nicht jedes KI-Tool löst eine Zustimmungspflicht aus. § 97 ArbVG regelt Bereiche, in denen der Betriebsrat ein Beratungsrecht hat — das Unternehmen muss informieren und konsultieren, hat aber das letzte Wort.

Ein Beispiel: Ein KI-Schreibassistent, der Textentwürfe erstellt und keine Nutzungsdaten speichert oder auswertet, fällt in der Regel unter § 97. Der Betriebsrat muss rechtzeitig informiert werden, kann Stellungnahmen abgeben — aber nicht blockieren.

Die Grenze zwischen § 96 und § 97 ist im Einzelfall nicht immer eindeutig. Entscheidend ist die tatsächliche Funktionsweise des Tools, nicht die Herstellerbeschreibung.

Welche Mitarbeiterdaten sind „kritisch“ – eine klare Abgrenzung

Nicht jede Dateneingabe in ein KI-Tool ist gleich problematisch. Eine strukturierte Einordnung hilft, den Handlungsbedarf schnell zu erkennen.

Kategorie 1: Name und Kontaktdaten Beispiel: Mitarbeitername in einer Angebotsvorlage. Niedrige Sensitivität im ArbVG-Sinne, aber trotzdem DSGVO-relevant — insbesondere wenn die Daten an Server außerhalb der EU übertragen werden.

Kategorie 2: Leistungs- und Produktivitätsdaten Beispiel: Anzahl bearbeiteter Tickets, Verkaufszahlen, Projektfortschritte. Mittlere Sensitivität — sobald diese Daten einem bestimmten Mitarbeiter zugeordnet werden können, ist das ArbVG relevant.

Kategorie 3: Kommunikationsdaten Beispiel: E-Mail-Verläufe, Chatprotokolle, Besprechungsaufzeichnungen. Hohe Sensitivität — hier greifen sowohl § 96 ArbVG als auch erhöhte DSGVO-Anforderungen. Das Thema DSGVO-konforme Meeting-Tools ist dabei eng verwandt: DSGVO-konforme Meeting-Aufzeichnung für KMU.

Kategorie 4: Gesundheitsdaten und besondere Kategorien (Art. 9 DSGVO) Beispiel: Krankenstandstage, ärztliche Atteste, Behinderungen. Höchste Sensitivität — für diese Daten gelten nach Art. 9 DSGVO besondere Schutzpflichten, eine einfache Einwilligung reicht nicht aus.

DATENKATEGORIE	DSGVO-GRUNDLAGE	ARBVG-RELEVANZ	HANDLUNGSBEDARF
Name / Kontakt	Art. 6 Abs. 1 lit. b	Gering	AVV prüfen
Leistungsdaten	Art. 6 Abs. 1 lit. f	Mittel	§ 96/97 prüfen
Kommunikation	Art. 6 Abs. 1 lit. a/f	Hoch	BV erforderlich
Gesundheit / Art. 9	Art. 9 Abs. 2	Sehr hoch	BV + explizite <u>Rechtsgrundlage</u>

Praktische Faustformel: Könnte diese Dateneingabe genutzt werden, um das Verhalten oder die Leistung eines Mitarbeiters zu bewerten oder zu kontrollieren? Wenn ja, muss der Betriebsrat einbezogen werden.

Wenn KI-Tools nicht nur Daten empfangen, sondern auch aktiv auf Unternehmenssysteme zugreifen, entsteht ein weiteres Risikobild — wie Sie den Datenzugriff von KI-Agenten kontrollieren, erfahren Sie in diesem Artikel: KI-Agenten Datenzugriff kontrollieren: KMU-Guide.

Das Praxis-Szenario – Was passiert, wenn ein Mitarbeiter echte Daten in ChatGPT eingibt?

Stellen wir ein konkretes Szenario durch: Eine HR-Managerin lädt eine Excel-Liste mit Mitarbeiternamen, Krankenstandstagen und Leistungsbeurteilungen in ein ChatGPT-Plugin, um eine Übersicht für das Jahresgespräch zu erstellen. Was auf den ersten Blick wie eine smarte Zeitersparnis wirkt, öffnet auf drei Ebenen rechtliche Probleme.

Ebene 1: DSGVO ChatGPT wird von OpenAI betrieben — einem US-amerikanischen Unternehmen. Eine Datenweitergabe in die USA ist nach aktuellem Datenschutzrecht nur zulässig, wenn ein Angemessenheitsbeschluss, Standardvertragsklauseln oder ein Auftragsverarbeitungsvertrag (AVV) vorliegen. Ohne AVV mit OpenAI ist die Datenweitergabe ein Verstoß gegen Art. 28 DSGVO — unabhängig davon, ob die Daten „nur kurz“ dort verarbeitet wurden. Einen vertieften Überblick zur DSGVO-konformen Nutzung von ChatGPT bietet dieser Artikel: DSGVO & ChatGPT im Unternehmen: Was gilt 2026?

Ebene 2: ArbVG Die Liste enthält Leistungsbeurteilungen und Krankenstandstage — beides Datenkategorien, bei denen ein Kontrollpotenzial besteht. Wurde der Betriebsrat informiert? Liegt eine Betriebsvereinbarung vor, die diese Art der Datenverarbeitung regelt? Wenn nicht, ist die Maßnahme nach § 96 ArbVG rechtsunwirksam.

Ebene 3: Haftung Bei einem DSGVO-Verstoß haftet nicht die HR-Managerin persönlich, sondern das Unternehmen als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Die Geschäftsführung ist verpflichtet, durch technische und organisatorische Maßnahmen (TOMs) sicherzustellen, dass solche Vorfälle nicht auftreten — also durch klare Nutzungsrichtlinien, Schulungen und geprüfte Tool-Verträge.

Dieser Artikel gibt die Leitfragen vor. Für eine rechtssichere Einschätzung Ihrer konkreten Situation ist anwaltliche Beratung unerlässlich.

Betriebsvereinbarung vs. Einzelzustimmung – der österreichische Unterschied

In Österreich gilt: Wo das ArbVG eine Betriebsvereinbarung vorschreibt, kann diese nicht durch individuelle Einwilligungen der betroffenen Mitarbeiter ersetzt werden. Das ist ein wesentlicher Unterschied zu Ländern ohne gesetzlich verankerte Betriebsratsmitbestimmung.

Eine datenschutzrechtliche Information nach § 13 DSG (österreichisches Datenschutzgesetz) oder eine DSGVO-Datenschutzerklärung ersetzt die Betriebsvereinbarung nicht. Sie sind ergänzend erforderlich, aber nicht ausreichend.

Wann ist eine Betriebsvereinbarung Pflicht? – Bei kontrollierenden oder überwachenden KI-Systemen (§ 96 ArbVG): immer – Bei Systemen mit indirektem Kontrollpotenzial: stark empfehlenswert, auch wenn formal „nur“ Beratungsrecht gilt

Was muss eine Betriebsvereinbarung zu KI-Tools mindestens enthalten?

- **Zweck des Tools:** Welches Ziel wird mit dem Einsatz verfolgt?
- **Erfasste Daten:** Welche Mitarbeiterdaten werden verarbeitet — direkt oder indirekt?
- **Zugriffsberechtigungen:** Wer im Unternehmen hat Zugang zu den Auswertungen?
- **Löschfristen:** Wie lange werden Daten gespeichert, wann werden sie gelöscht?
- **Kontrollverbot:** Explizite Regelung, dass das Tool nicht zur individuellen Leistungskontrolle genutzt wird — oder wenn doch, unter welchen Bedingungen.

Die Arbeiterkammer Österreich stellt Musterbetriebsvereinbarungen bereit, die als Ausgangsbasis dienen können. Diese finden sich unter www.arbeiterkammer.at — eine direkte Verlinkung auf die jeweils aktuelle Musterversion empfiehlt sich, da diese regelmäßig aktualisiert werden.

Für die interne Dokumentation und Ablage Ihrer KI-Richtlinie eignen sich DSGVO-konforme Wissensmanagement-Tools — einen Vergleich gängiger Optionen finden Sie hier: Alternativen zu Notion: Tools für Notizen, Wikis und Wissensmanagement.

Was tun, wenn es keinen Betriebsrat gibt?

In österreichischen KMU unter fünf Mitarbeitern besteht keine gesetzliche Pflicht zur Errichtung eines Betriebsrats — und viele mittelgroße Unternehmen haben schlicht keinen aktiven. Ohne Betriebsrat entfällt die Mitbestimmungspflicht nach ArbVG.

Das bedeutet aber nicht, dass gar nichts geregelt werden muss. Die DSGVO-Pflichten gelten vollumfänglich weiter: Zweckbindung, Informationspflicht gegenüber betroffenen Mitarbeitern, AVV mit dem Tool-Anbieter, Dokumentation im Verarbeitungsverzeichnis. Diese Regelungen sollten in Arbeitsverträgen oder einer internen Datenschutzrichtlinie verankert sein.

Schritt-für-Schritt – So setzt ein Betriebsrat eine KI-Richtlinie auf

Der folgende Prozess ist für österreichische KMU mit bestehendem Betriebsrat konzipiert. Er orientiert sich an der gängigen Praxis — nicht an einem juristischen Idealmodell.

- 1. Bestandsaufnahme: Welche KI-Tools werden bereits genutzt?** Erfassen Sie alle eingesetzten KI-Tools — auch inoffizielle, die Mitarbeiter eigenständig nutzen (z. B. ChatGPT, Copilot, KI-Übersetzungstools). Erfahrungsgemäß ist die Dunkelziffer hoch.
- 2. Kategorisierung: Kontrollierend oder rein assistierend?** Für jedes Tool die zentrale Frage beantworten: Kann es Mitarbeiterdaten erfassen, auswerten oder aggregieren? Wenn ja, ist es potenziell kontrollierend.
- 3. Rechtliche Einordnung: § 96 oder § 97 ArbVG?** Tools mit Kontrollpotenzial fallen unter § 96 (Zustimmungspflicht). Rein assistierende Tools ohne Mitarbeiterdatenbezug fallen unter § 97 (Beratungsrecht). Im Zweifel: rechtliche Beratung einholen.
- 4. Verhandlung: Nicht verhandelbare Mindestinhalte definieren** Kontrollverbot, Transparenzpflicht gegenüber Mitarbeitern und Löschfristen sind typischerweise nicht verhandelbar. Diese Punkte sollten vom Betriebsrat als Mindestbedingungen definiert werden.
- 5. Entwurf der Betriebsvereinbarung** Als Startpunkt eignen sich die Musterbetriebsvereinbarungen der AK Österreich. Der Entwurf sollte die im vorigen Abschnitt genannten Mindestinhalte vollständig abdecken.
- 6. Schulung der Mitarbeiter: Wer darf was eingeben?** Eine Betriebsvereinbarung regelt das Framework — die gelebte Praxis entscheidet über ihre Wirksamkeit. Mitarbeiter müssen verstehen, welche Daten sie in welche Tools eingeben dürfen und welche nicht. Das gilt besonders für externe KI-Dienste wie ChatGPT.
- 7. Laufende Kontrolle: Wie wird Einhaltung geprüft?** Einmalige Regelungen reichen nicht. Legen Sie fest, wie häufig die Nutzungsrichtlinie überprüft wird (z. B. jährlich oder bei Einführung neuer Tools) und wer dafür zuständig ist.

Haftung und Konsequenzen – was droht bei Verstößen?

Szenario 1: Unternehmen führt KI-Tool ohne Betriebsvereinbarung ein Nach § 96 ArbVG ist die Maßnahme rechtsunwirksam. Der Betriebsrat kann beim zuständigen Gericht auf Unterlassung klagen. Das Unternehmen muss das Tool abschalten oder außer Betrieb nehmen, bis eine rechtskonforme Vereinbarung vorliegt. Zusätzlich entsteht Konfliktpotenzial, das den Betriebsfrieden langfristig belastet.

Szenario 2: Mitarbeiter gibt sensible Daten in externes KI-Tool ein – ohne Regelung Ein Verstoß gegen Art. 28 DSGVO (fehlender AVV) oder Art. 9 DSGVO (besondere Datenkategorien) ist meldepflichtig. Nach Art. 33 DSGVO muss die österreichische Datenschutzbehörde (DSB) innerhalb von 72 Stunden informiert werden, wenn eine Datenpanne ein Risiko für betroffene Personen darstellt. Art. 34 DSGVO verpflichtet unter Umständen zur direkten Information der betroffenen Mitarbeiter. Die möglichen Bußgelder betragen bis zu 4 % des weltweiten Jahresumsatzes oder 20 Millionen Euro – je nachdem, was höher ist.

Zuständige Aufsichtsbehörde in Österreich ist die Datenschutzbehörde (DSB), nicht das deutsche BayLDA oder der Bundesbeauftragte für den Datenschutz.

Für KMU ist das Bußgeldrisiko in der Praxis oft geringer als das Reputationsrisiko und das Konfliktpotenzial mit dem Betriebsrat. Ein eskalierter Betriebsrat-Konflikt nach einer unregelmäßigen Tool-Einführung kann den Betriebsablauf monatelang belasten – und lässt sich durch frühzeitige Einbindung nahezu vollständig vermeiden.

Das Risiko durch externe KI-Tools endet nicht bei der DSGVO – auch Angriffsvektoren wie KI-gestützte Ransomware nutzen schlecht gesicherte Tool-Zugänge aus: KI-automatisierte Ransomware: Risiken für KMU.

Praxis-Tipp – KI-Tool-Einführung ohne Rechtsstreit: So gehen KMU vor

Bei Strukturaflow sehen wir regelmäßig, dass die rechtliche Seite der KI-Einführung zum eigentlichen Blocker wird – nicht die Technologie. Unternehmen haben ein Tool gefunden, das ihre Prozesse verbessern würde, wissen aber nicht, ob sie es einsetzen dürfen, ohne Konflikte zu riskieren.

Der häufigste Fehler: Das Tool wird eingeführt, der Betriebsrat wird nachträglich informiert – und lehnt ab. Dann beginnt eine Rückabwicklung, die Zeit und Vertrauen kostet.

Drei typische Versäumnisse, die sich vermeiden lassen: – AVV vergessen: Viele Cloud-Tools verarbeiten Daten auf Servern außerhalb der EU. Ohne geprüften Auftragsverarbeitungsvertrag ist jede Nutzung mit personenbezogenen Daten rechtswidrig. – **Kein Verwendungszweck definiert**:

Was das Tool können soll, muss dokumentiert sein — nicht nur für den Betriebsrat, sondern auch für die eigene DSGVO-Dokumentation. – **Mitarbeiter nicht informiert:** Auch wenn alles rechtlich korrekt geregelt ist, entsteht Misstrauen, wenn Mitarbeiter nicht wissen, welche Daten wie verarbeitet werden.

Die Empfehlung für die Praxis: Klären Sie vor der Tool-Auswahl, welche Datenkategorien das Tool verarbeiten wird. Binden Sie den Betriebsrat dann frühzeitig ein — nicht als Pflichtübung, sondern als Partner, der die Umsetzung im Betrieb erleichtert. Ein Betriebsrat, der von Anfang an mitgedacht hat, wird eine Betriebsvereinbarung nicht blockieren, sondern aktiv mittragen.

Nächste Schritte

Drei Maßnahmen, die jetzt sinnvoll sind — unabhängig von der Betriebsgröße:

1. **Bestandsaufnahme der genutzten KI-Tools** — auch der inoffiziellen, die Mitarbeiter selbst einsetzen
2. **Prüfung, ob eine Betriebsvereinbarung besteht oder nötig ist** — anhand der Kategorisierung kontrollierend vs. assistierend
3. **Interne KI-Nutzungsrichtlinie erstellen** — wer darf welche Daten in welche Tools eingeben, und unter welchen Bedingungen

Wenn Sie gerade dabei sind, KI-Tools in Ihrem Unternehmen einzuführen, und unsicher sind, wo Ihr konkretes Risiko liegt — genau dafür ist das Beratungsgespräch bei Strukturaflow gedacht. In einem unverbindlichen 30-Minuten-Gespräch schauen wir uns Ihre konkrete Situation an: welche Tools Sie nutzen oder einführen möchten, welche Datenkategorien betroffen sind, und ob Ihr Betriebsrat bereits eingebunden ist oder eingebunden werden muss.

Häufige Fragen

Muss der Betriebsrat bei jedem KI-Tool zustimmen? Nein — nur bei Tools, die zur Kontrolle oder Überwachung von Mitarbeitern geeignet sind (§ 96 ArbVG). Rein assistierende Tools ohne Kontrollpotenzial fallen unter das Beratungsrecht nach § 97 ArbVG, wo der Betriebsrat informiert und konsultiert werden muss, aber nicht zustimmen muss.

Was gilt, wenn unser Unternehmen keinen Betriebsrat hat? Dann entfällt die Mitbestimmungspflicht nach ArbVG. DSGVO-Pflichten — Informationspflicht, Zweckbindung, AVV mit dem Anbieter — gelten jedoch uneingeschränkt weiter und müssen über Arbeitsverträge oder eine interne Datenschutzrichtlinie geregelt sein.

Dürfen Mitarbeiter Kundendaten in ChatGPT eingeben? In der Regel nein. Ohne geprüften Auftragsverarbeitungsvertrag mit OpenAI und ohne definierte Nutzungsrichtlinie ist das ein Verstoß gegen Art. 28 DSGVO. Die Haftung liegt beim Unternehmen als Verantwortlichem, nicht beim einzelnen Mitarbeiter.

Was kostet eine fehlende Betriebsvereinbarung konkret? Rechtlich: Die Maßnahme ist unwirksam, der Betriebsrat kann auf Unterlassung klagen — das Unternehmen muss das Tool abschalten. Finanziell: Zusätzlich drohen DSGVO-Bußgelder durch die österreichische Datenschutzbehörde von bis zu 4 % des weltweiten Jahresumsatzes oder 20 Millionen Euro — je nach Schwere des Verstoßes. In der Praxis österreichischer KMU wiegt der Vertrauensverlust gegenüber dem Betriebsrat oft schwerer als das Bußgeld selbst.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

<https://wissen.strukturaflow.it.com>