

COMPLIANCE

KI-Tools zur Mitarbeiterüberwachung: Was ist in Deutschland erlaubt?

KI-Monitoring im Betrieb: Was DSGVO, BDSG §26 und BetrVG §87 erlauben — mit Tabelle, Entscheidungsbaum und Muster-Betriebsvereinbarung.

AUTOR

Strukturaflow-Team

VERÖFFENTLICHT

6. Mai 2026

ONLINE LESEN

<https://wissen.strukturaflow.it.com/ki-tool-mitarbeiterueberwachung-dsgvo-deutschland-erlaubt/>

Ein KMU führt ein KI-gestütztes Activity-Tracking-Tool ein — und noch vor dem Go-Live stellt der Betriebsrat die Frage: „Darf das überhaupt so eingesetzt werden?“ Dieses Unbehagen ist berechtigt. Weder ist KI-Monitoring in Deutschland pauschal verboten, noch gilt dafür ein Freifahrtsschein.

Entscheidend sind drei Faktoren: eine tragfähige Rechtsgrundlage, das Prinzip der Verhältnismäßigkeit und die rechtzeitige Einbindung der Mitbestimmung. Fehlt einer dieser Bausteine, riskieren Unternehmen nicht nur Bußgelder, sondern auch Beweisverwertungsverbote und Unterlassungsklagen.

Dieser Artikel erklärt, welche Gesetze gleichzeitig gelten, was der Betriebsrat mitentscheiden muss, welche KI-Funktionen konkret erlaubt oder unzulässig sind — und wie eine rechtssichere Einführung Schritt für Schritt aussieht. Er richtet sich an HR-Verantwortliche, Geschäftsführer und Datenschutzbeauftragte in deutschen KMU, die mit KI-gestützten Tools zur Zeiterfassung, Produktivitätsmessung oder Qualitätskontrolle arbeiten oder dies planen.

Rechtlicher Rahmen: Welche Gesetze gelten gleichzeitig?

KI-Monitoring im Arbeitsverhältnis berührt nicht ein Gesetz, sondern mehrere — die unterschiedliche Ebenen abdecken und sich gegenseitig begrenzen.

DSGVO (Art. 5, 6, 9, 22): Gibt die europäischen Grundsätze vor: Zweckbindung, Datensparsamkeit, Rechtmäßigkeit der Verarbeitung und — besonders relevant — das Verbot vollautomatisierter Einzelentscheidungen ohne menschliche Überprüfung.

BDSG §26: Der Beschäftigtendatenschutz nach deutschem Bundesdatenschutzgesetz ist für den Arbeitskontext die speziellere Norm und geht den allgemeinen DSGVO-Öffnungsklauseln vor. §26 erlaubt die Datenverarbeitung, wenn sie für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Das Wort „erforderlich“ ist dabei kein Füllwort — Gerichte prüfen es genau.

BetrVG §87 Abs. 1 Nr. 6: Zwingendes Mitbestimmungsrecht des Betriebsrats bei der Einführung und Anwendung technischer Einrichtungen, die geeignet sind, Verhalten oder Leistung der Arbeitnehmer zu überwachen. Dieses Recht ist nicht abdingbar.

NORM	REGELT WAS?	FÜR WEN RELEVANT?
DSGVO Art. 6 / Art. 22	Rechtmäßigkeit der Verarbeitung, Verbot vollautomatisierter Entscheidungen	Alle verarbeitenden Stellen
BDSG §26	Beschäftigtendatenschutz als Spezialregelung	Arbeitgeber in Deutschland
BetrVG §87 Nr. 6	Mitbestimmung bei technischer Überwachung	Betriebe mit Betriebsrat
Art. 35 DSGVO	Datenschutz-Folgenabschätzung	Pflicht bei systematischer Überwachung

Ab 2025/2026 kommt eine weitere Dimension hinzu: Der [EU AI Act](#) klassifiziert bestimmte KI-Systeme im Personalbereich als „hochriskant“ — darunter fallen Tools zur Bewertung von Mitarbeitenden. Das schafft zusätzliche Transparenz- und Dokumentationspflichten.

Was macht KI-Monitoring rechtlich anders als klassische Tools?

Eine Stechuhr zeichnet auf, wann jemand kommt und geht. Ein KI-Tool kann aus denselben Zeitstempeln plus Aktivitätsdaten einen „Engagement-Score“ berechnen, Verhaltensanomalien erkennen oder Rückschlüsse auf Pausen, Konzentrationsphasen und Produktivitätsschwankungen ziehen.

Diese Inferenz-Fähigkeit ist das entscheidende rechtliche Unterscheidungsmerkmal. Die KI zieht Schlüsse, die über die ursprünglich erhobenen Daten hinausgehen — das ist eine andere rechtliche Kategorie als die bloße Erfassung von Rohdaten. [Art. 22 DSGVO](#) adressiert genau das: Automatisierte Einzelentscheidungen, die rechtliche oder ähnlich erhebliche Auswirkungen auf Personen haben, sind grundsätzlich unzulässig, sofern keine Ausnahme greift und keine menschliche Überprüfung stattfindet.

Ein Beispiel aus der Praxis: Ein Keystroke-Logger ist aus Arbeitnehmersicht unangenehm. Ein KI-Tool, das aus Tastatureingaben, Mausbewegungen und App-Nutzung einen Produktivitätsscore ableitet und diesen automatisch für Personalentscheidungen verwendet, ist eine fundamental andere rechtliche Situation.

Was darf ein KI-Tool im Arbeitskontext konkret messen – und was nicht?

Die folgende Tabelle gibt einen strukturierten Überblick. Wichtig: „Grundsätzlich erlaubt“ bedeutet nicht „ohne Vorbereitung einsetzbar“ — die Voraussetzungsspalte ist Teil der Zulässigkeit.

FUNKTION	ZULÄSSIGKEIT	VORAUSSETZUNG
Zeiterfassung (ArbZG-konform)	□ Grundsätzlich erlaubt	Transparenz, Betriebsvereinbarung empfohlen
Produktivitäts-Scoring auf Basis von Klicks/Aktivität	△ Nur eingeschränkt	Kein Echtzeit-Monitoring einzelner Personen, keine individuelle Auswertung ohne Betriebsvereinbarung
E-Mail-Inhalte KI-gestützt scannen	□ In der Regel unzulässig	Ausnahme: begründeter Straftatverdacht, strenge formale Anforderungen
KI-Qualitätskontrolle von Kundengesprächen (Call Center)	△ Möglich	Explizite Mitarbeiterinformation, Betriebsvereinbarung, keine Totalüberwachung
Anonymisiertes Team-Reporting (keine Einzelauswertung)	□ Eher unkritisch	Echte <u>Anonymisierung</u> technisch sichergestellt
Standorttracking im Außendienst	△ Eingeschränkt	Verhältnismäßigkeit, Dienstzweck nachweisbar, Betriebsvereinbarung sinnvoll
Biometrische Erkennung (Gesicht, Stimme)	□ Verboten ohne Ausnahmeregelung	Art. 9 DSGVO, besondere Kategorie personenbezogener Daten

Zu Produktivitäts-Scoring: Ein mittelständisches Softwareunternehmen, das über ein Activity-Monitoring-Tool sehen möchte, ob Projekte gleichmäßig ausgelastet sind, kann aggregierte Team-Daten nutzen. Sobald aber einzelne Mitarbeitende mit Namen und Score in einem Dashboard erscheinen, ist ohne Betriebsvereinbarung die Grenze zur unzulässigen Verhaltenskontrolle überschritten.

Zu KI-Call-Analytics: Tools wie Gong oder Chorus fallen in eine besonders regulierte Zone, weil sie nicht nur Mitarbeitende, sondern auch Kunden erfassen. Hier brauchen Sie neben der internen Betriebsvereinbarung auch eine rechtlich abgesicherte Information gegenüber Gesprächspartnern – ein einfacher Hinweiston genügt dafür in der Regel nicht.

Zu Standorttracking: Ein Lieferdienst, der Fahrtrouten für die Tourenplanung erfasst, hat einen klar nachweisbaren Dienstzweck. Lückenlose Bewegungsprofile außerhalb der Arbeitszeit oder minutengenaues Tracking ohne sachlichen Grund sind damit nicht gedeckt.

Der Grundsatz der Verhältnismäßigkeit – einfach erklärt

BDSG §26 erlaubt nur, was zur Erreichung des Zwecks „erforderlich“ ist. Juristen prüfen das mit einem Dreistufentest:

1. **Geeignetheit:** Ist das Tool überhaupt geeignet, den angestrebten Zweck zu erreichen?
2. **Erforderlichkeit:** Gibt es ein milderes Mittel, das denselben Zweck ebenso gut erfüllt?
3. **Angemessenheit:** Stehen der Eingriff in die Rechte der Mitarbeitenden und der Nutzen des Arbeitgebers in einem vernünftigen Verhältnis?

Ein Beispiel: Ein KMU möchte die Qualität seiner Support-Tickets sichern. Ein KI-Tool, das jeden Tastendruck des Support-Teams aufzeichnet, wäre zur Qualitätssicherung zwar geeignet – aber nicht erforderlich. Stichprobenbasiertes anonymisiertes Monitoring der Ticket-Inhalte wäre ein milderes Mittel. Das vollständige Keystroke-Logging würde den Verhältnismäßigkeitstest nicht bestehen.

Betriebsrat und Mitbestimmung: §87 BetrVG ist kein optionales Extra

§87 Abs. 1 Nr. 6 BetrVG gibt dem Betriebsrat ein zwingendes Mitbestimmungsrecht bei der Einführung und Anwendung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen. Das Wort „geeignet“ ist entscheidend: Es kommt nicht darauf an, ob der Arbeitgeber das Tool zur Überwachung einsetzen will – sondern ob es technisch dazu geeignet ist.

KI-Tools zur Zeiterfassung, Produktivitätsmessung, Call-Analyse oder Activity-Monitoring fallen fast ausnahmslos darunter. Das gilt auch dann, wenn der Anbieter das Produkt als „Engagement-Tool“ oder „HR-Analytics-Plattform“ vermarktet.

Die Konsequenzen fehlender Mitbestimmung sind erheblich: Der Betriebsrat kann die Unterlassung des Tool-Einsatzes verlangen. Darüber hinaus hat das Bundesarbeitsgericht in einer Grundsatzentscheidung (BAG, 2 AZR 371/21, 27. Juli 2021) festgehalten, dass rechtswidrig durch verdeckte Überwachung gewonnene Daten einem Beweisverwertungsverbot unterliegen können – im Klartext: Wer einen Mitarbeitenden auf Basis unzulässig erhobener KI-Daten abmahnt oder kündigt, riskiert, diesen Beweis vor Gericht nicht einsetzen zu dürfen.

Was gilt in Betrieben ohne Betriebsrat? Hier gibt es keine formale Mitbestimmungspflicht. Dennoch sollten Arbeitgeber eine schriftliche Mitarbeiterinformation erstellen, eine Interessenabwägung dokumentieren und Einwilligungen – wo rechtlich sinnvoll – einholen. Allerdings: Einwilligungen im Arbeitsverhältnis sind rechtlich problematisch, weil die Freiwilligkeit aufgrund des Machtgefälles zwischen Arbeitgeber und Arbeitnehmer schwer nachweisbar ist. Das Bundesarbeitsgericht und die Datenschutzbehörden sehen das kritisch. Eine Einwilligung ersetzt deshalb keine solide Rechtsgrundlage nach BDSG §26.

Muster-Regelungspunkte für eine Betriebsvereinbarung (KI-Monitoring)

Eine Betriebsvereinbarung zu KI-Tools sollte mindestens sieben Punkte abdecken:

1. **Konkrete Tool-Benennung:** Welches System mit welchen aktivierten Funktionen wird eingesetzt? Nicht „ein KI-Produktivitätstool“, sondern: Produktname, Version, genutzte Module.
2. **Zweck und Verwendungsrahmen:** Wofür dürfen die erhobenen Daten ausgewertet werden — und ausdrücklich wofür nicht.
3. **Speicherdauer und Löschfristen:** Wann werden Rohdaten gelöscht? Wann aggregierte Auswertungen?
4. **Zugriffsberechtigung nach Rollen:** Wer darf was sehen — HR-Leitung, Teamleiter, Geschäftsführung, IT-Administration?
5. **Ausschluss individueller Echtzeit-Auswertung:** Explizite Regelung, dass keine personenbezogene Echtzeit-Dashboards ohne Zustimmung betrieben werden.
6. **Informationspflicht gegenüber Beschäftigten:** Wie, wann und in welcher Form werden Mitarbeitende informiert?
7. **Revisionsmechanismus:** Jährliche gemeinsame Überprüfung, ob die Betriebsvereinbarung noch dem tatsächlichen Tool-Einsatz entspricht.

Wichtiger Hinweis: Diese Punkte sind ein strukturierter Ausgangspunkt, kein fertiges Rechtsdokument. Für eine verbindliche Betriebsvereinbarung sollte ein auf Arbeitsrecht spezialisierter Anwalt hinzugezogen werden — insbesondere weil die konkreten Formulierungen über Rechtswirksamkeit entscheiden.

Entscheidungsbaum: Ist mein KI-Monitoring-Use-Case erlaubt?

Bevor ein Tool evaluiert oder beschafft wird, lohnt sich dieser strukturierte Selbsttest:

Frage 1: Werden personenbezogene Daten von Beschäftigten verarbeitet? – Nein → DSGVO und BDSG §26 nicht unmittelbar anwendbar. Trotzdem Pseudonymisierung prüfen. – Ja → Weiter zu Frage 2.

Frage 2: Gibt es einen legitimen Zweck nach BDSG §26 (Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses)? – Nein → Verarbeitung unzulässig. Tool-Einsatz in dieser Form nicht möglich. – Ja → Weiter zu Frage 3.

Frage 3: Ist das Mittel verhältnismäßig — gibt es kein milderes Mittel, das denselben Zweck erfüllt? – Nein → Verarbeitung unzulässig. Funktionsumfang des Tools reduzieren oder Alternative suchen. – Ja → Weiter zu Frage 4.

Frage 4: Gibt es im Betrieb einen Betriebsrat? – Nein → Schriftliche Mitarbeiterinformation erstellen, Interessenabwägung dokumentieren, Verarbeitungsverzeichnis aktualisieren. – Ja → Mitbestimmungsverfahren nach §87 BetrVG einleiten, bevor das Tool auch nur in einer Testumgebung mit echten Mitarbeiterdaten betrieben wird.

Frage 5: Trifft das Tool automatisierte Einzelentscheidungen mit erheblichen Auswirkungen (z. B. Score-basierte Abmahnungen, automatische Leistungsbeurteilungen)? – Ja → Art. 22 DSGVO greift. Menschliche Überprüfung zwingend vorschalten, Betroffenenrechte implementieren, DSFA wahrscheinlich erforderlich. – Nein → Dokumentation vervollständigen und Go-Live vorbereiten.

Checkliste vor Go-Live — diese fünf Dokumente müssen vorliegen: 1. Zweckbeschreibung (schriftlich, intern freigegeben) 2. Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO 3. Betriebsvereinbarung oder dokumentierte Mitarbeiterinformation 4. Auftragsverarbeitungsvertrag (AVV) mit dem Tool-Anbieter 5. Aktualisierter Eintrag im Verarbeitungsverzeichnis

Aktuelle Rechtsprechung: Was die Gerichte entschieden haben

BAG 2 AZR 371/21 (27. Juli 2021): In diesem Grundsatzurteil hat das Bundesarbeitsgericht entschieden, dass Daten aus einem Keylogger — der ohne Kenntnis des Betriebsrats eingesetzt wurde — einem Beweisverwertungsverbot unterliegen. Der Arbeitgeber konnte den Mitarbeitenden deshalb trotz nachgewiesener Pflichtverletzung nicht wirksam kündigen. Die Botschaft an KMU ist klar: Rechtswidrig erhobene Daten helfen im Streitfall nicht — sie können die eigene Rechtsposition sogar verschlechtern.

Zum EU AI Act (ab 2025/2026): Der EU AI Act stuft KI-Systeme zur Bewertung von Arbeitnehmern als hochriskant ein. Das bedeutet: Transparenzpflichten, Pflicht zur menschlichen Aufsicht und vorgeschriebene Konformitätsbewertungen. Wer heute ein solches System einführt, sollte die Anforderungen bereits mitdenken — auch wenn die Übergangspflichten gestaffelt gelten.

Praxisrelevante Lektion am Beispiel Microsoft Viva Insights: Das Tool bietet in der Grundkonfiguration aggregierte Auswertungen ohne Einzelpersonenbezug. Sobald aber Manager-Reports aktiviert werden, die einzelne Mitarbeitende zeigen, ist die Schwelle zum mitbestimmungspflichtigen Monitoring überschritten. Die DSGVO-Stellungnahmen von Microsoft beschreiben, wie das Tool konfiguriert werden muss — diese Konfiguration muss dann auch tatsächlich umgesetzt und in der Betriebsvereinbarung festgehalten werden.

Wichtiger Hinweis: Urteile und Behördenpositionen entwickeln sich weiter. Dieser Abschnitt sollte zum Zeitpunkt der Veröffentlichung auf aktuelle Entscheidungen hin geprüft werden.

Welche KI-Tools werden aktuell eingesetzt – und wie stehen sie da?

Statt einer vollständigen Tool-Liste, die schnell veraltet, ist eine Einordnung nach Tool-Kategorien hilfreicher:

□ **Zeiterfassung mit KI-Projektzuordnung** (automatische Buchung auf Kostenstellen, intelligente Vorschläge): Grundsätzlich datenschutzfreundlich, wenn die Zuordnung durch den Mitarbeitenden bestätigt wird. Betriebsvereinbarung empfohlen, aber keine hohe Risikoklasse. Handlungsempfehlung: Einführung mit AVV und Mitarbeiterinformation, bei vorhandenem Betriebsrat kurze Abstimmung.

□ **Activity Monitoring** (z. B. Microsoft Viva Insights, Hubstaff, ActivTrak): Stark konfigurationsabhängig. In der restriktivsten Einstellung (nur aggregierte Team-Daten) eher unkritisch. Mit aktivierten Einzel-Dashboards oder Echtzeit-Überwachung sofort mitbestimmungspflichtig. Kritische Funktionen im Anbieter-Interface klar benennen und in der Betriebsvereinbarung explizit ausschließen oder einschränken. DSGVO-Stellungnahmen und AVV des Anbieters zwingend prüfen.

□ **KI-gestützte Call-Recording und -Analyse** (z. B. Gong, Chorus): Hohe Anforderungen auf zwei Ebenen – gegenüber Mitarbeitenden (Betriebsvereinbarung, explizite Information) und gegenüber Kunden (Hinweispflichten, Einwilligung oder berechtigtes Interesse mit Interessenabwägung). Wer diese Tools ohne vollständiges Compliance-Paket betreibt, riskiert Bußgelder durch Datenschutzbehörden. Handlungsempfehlung: Vor Einführung Datenschutzbeauftragten einbinden.

□ **Anomalie-Erkennung und Insider-Threat-Tools**: Höchste Risikoklasse. Diese Tools analysieren systematisch Verhaltensabweichungen einzelner Mitarbeitender. In KMU fehlt dafür in aller Regel die Verhältnismäßigkeitsgrundlage – der Aufwand für rechtssichere Implementierung übersteigt den Nutzen deutlich. Handlungsempfehlung: In KMU bis 250 Mitarbeitende in der Regel nicht einsetzbar ohne erhebliche rechtliche Absicherung.

Was Sie vom Anbieter verlangen müssen

Unabhängig vom konkreten Tool gelten folgende vertragliche Mindestanforderungen:

AVV nach Art. 28 DSGVO: Pflicht – kein Tool darf ohne abgeschlossenen Auftragsverarbeitungsvertrag eingesetzt werden. Viele Anbieter stellen diesen auf Anfrage oder als Self-Service-Dokument bereit. Mehr zu den Grundlagen finden Sie im Artikel DSGVO & ChatGPT im Unternehmen, der den AVV-Prozess allgemein erklärt.

Speicherort der Daten: EU-Server oder Drittland? Bei US-Anbietern ist die Schrems-II-Problematik zu beachten – prüfen Sie, ob Standardvertragsklauseln (SCCs) vorliegen und ob der Anbieter dem US CLOUD Act unterliegt.

Technisch-organisatorische Maßnahmen (TOMs): Anfordern und dokumentieren. Welche Verschlüsselung, welche Zugriffskontrollen, welche Löschprozesse betreibt der Anbieter?

Subauftragnehmer-Liste: Welche weiteren Dienstleister erhält der Anbieter Zugriff? KI-Systeme laufen häufig auf Infrastruktur von Drittanbietern (AWS, Azure, Google Cloud) — auch das muss im AVV geregelt sein.

Praxis-Tipp: Rechtssichere Einführung in 6 Schritten

Viele KMU haben die technische Seite bereits im Blick — sie wissen, welches Tool sie wollen und was es kostet. Die rechtliche und prozessuale Vorbereitung bleibt dann oft bis kurz vor dem Go-Live liegen. Das ist der häufigste Fehler.

Schritt 1: Use-Case-Definition Was soll das Tool konkret leisten? Welche Daten werden erhoben, zu welchem Zweck, von welchen Personengruppen? Dieser Zweck muss schriftlich festgehalten werden — er ist Grundlage für alle weiteren Schritte und für die spätere Rechtmäßigkeitsprüfung.

Schritt 2: Datenschutz-Folgenabschätzung (DSFA) Bei systematischer Überwachung von Beschäftigten ist die DSFA nach Art. 35 DSGVO in der Regel verpflichtend — nicht optional. Sie analysiert Risiken für Betroffene und dokumentiert Schutzmaßnahmen. Ohne DSFA fehlt ein zentrales Pflichtdokument. Wenn noch kein KI-Audit im Unternehmen stattgefunden hat, bietet sich das als paralleler Schritt an.

Schritt 3: Betriebsrat frühzeitig einbinden Nicht nach der Kaufentscheidung, nicht parallel zur Implementierung — sondern vor der Tool-Evaluation. Der Betriebsrat hat das Recht, die Einführung zu verhindern. Wer ihn früh einbindet, schafft Vertrauen und vermeidet teure Rückabwicklungen.

Schritt 4: Betriebsvereinbarung abschließen Auf Basis der Muster-Regelungspunkte aus diesem Artikel eine individuelle Vereinbarung erarbeiten und rechtlich prüfen lassen. Bei fehlendem Betriebsrat: Mitarbeiterinformation dokumentieren, Interessenabwägung schriftlich festhalten.

Schritt 5: AVV mit Anbieter abschließen TOMs prüfen, Speicherort klären, Subauftragnehmer-Liste anfordern. Dieser Schritt gehört vor den Vertragsabschluss mit dem Anbieter — nicht danach.

Schritt 6: Verarbeitungsverzeichnis aktualisieren Das neue Tool als Verarbeitungstätigkeit aufnehmen. Angaben: Zweck, Datenkategorien, Empfänger, Löschfristen, technisch-organisatorische Maßnahmen. Dieser Eintrag ist kein einmaliger Aufwand — er muss bei jeder Funktionserweiterung des Tools aktualisiert werden.

Nächste Schritte

KI-Monitoring rechtssicher einzuführen, ist keine Aufgabe, die sich an einem Nachmittag erledigt — aber mit dem richtigen Vorgehen ist es für KMU gut zu bewältigen. Der kritische Punkt liegt Erfahrungsgemäß nicht im Verständnis der Rechtslage, sondern in der Übersetzung in konkrete Dokumente, Prozesse und Gespräche mit dem Betriebsrat oder den Mitarbeitenden.

Wenn Sie gerade dabei sind, ein Activity-Monitoring-, Zeiterfassungs- oder Call-Analytics-Tool zu evaluieren, oder wenn Sie bereits ein Tool im Einsatz haben und sich über die rechtliche Absicherung nicht sicher sind — ein unverbindliches Beratungsgespräch mit dem Strukturaflow-Team kann helfen, die offenen Punkte zu strukturieren. In 30 Minuten klären wir gemeinsam, wo bei Ihrem konkreten Use-Case die relevanten Risiken liegen und welche nächsten Schritte sinnvoll wären.

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>