

Muster-Betriebsvereinbarung: Einführung eines Online-Wächterkontrollsystems (OWKS) mit GPS-Ortung

Für Geschäftsführer von Sicherheitsdiensten und Betriebsräte

Teil 1: Einleitung und Verwendungshinweis

Warum eine Betriebsvereinbarung?

Ein Online-Wächterkontrollsystem (OWKS) erfasst systematisch, wann und wo Kontrollpunkte gescannt wurden, dokumentiert Ereignisse und kann – sofern aktiviert – die GPS-Position von Mitarbeitern während der Schicht anzeigen. Damit ist ein OWKS aus rechtlicher Sicht eine **technische Einrichtung, die dazu bestimmt (oder zumindest geeignet) ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen**.

Genau dafür sieht das Betriebsverfassungsgesetz eine **zwingende Mitbestimmung des Betriebsrats** vor:

§ 87 Abs. 1 Nr. 6 BetrVG: Der Betriebsrat hat mitzubestimmen bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen.“

Nach ständiger Rechtsprechung des Bundesarbeitsgerichts genügt dabei bereits die **objektive Eignung** zur Überwachung – auf eine Überwachungsabsicht des Arbeitgebers kommt es nicht an. Praktisch bedeutet das: **Existiert ein Betriebsrat, darf ein OWKS nicht ohne dessen Zustimmung eingeführt werden**. Führt der Arbeitgeber das System dennoch einseitig ein, kann der Betriebsrat die Unterlassung verlangen; zudem drohen Verwertungsverbote für so gewonnene Daten in arbeitsrechtlichen Auseinandersetzungen.

Die Betriebsvereinbarung (BV) ist dabei kein lästiges Hindernis, sondern **das Werkzeug, das beiden Seiten Sicherheit gibt**:

- **Für die Geschäftsführung:** Rechtssichere Einführung, klare Spielregeln, keine spätere Blockade, belastbare Rechtsgrundlage für die Datenverarbeitung, Nachweisfähigkeit gegenüber Auftraggebern und Aufsichtsbehörden.
- **Für den Betriebsrat und die Beschäftigten:** Verbindlich geregelte Zweckbindung, Auswertungsverbote, Löschrufen und Beschäftigtenrechte – schwarz auf weiß, einklagbar.

Verhältnis zum Datenschutzrecht (Art. 88 DSGVO, § 26 BDSG)

Mitbestimmung und Datenschutz sind **zwei getrennte Prüfungsebenen**, die beide erfüllt sein müssen:

1. **Art. 88 DSGVO** ist die Öffnungsklausel der DSGVO für den Beschäftigtendatenschutz. Sie erlaubt den Mitgliedstaaten und ausdrücklich auch **Kollektivvereinbarungen** (dazu zählen Betriebsvereinbarungen), spezifischere Regeln für die Verarbeitung von Beschäftigtendaten vorzusehen. Eine Betriebsvereinbarung kann damit selbst als Rechtsgrundlage für die Datenverarbeitung dienen – allerdings nur, wenn sie die Anforderungen des Art. 88 Abs. 2 DSGVO erfüllt: angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der Beschäftigten, insbesondere Transparenz der Verarbeitung. **Eine BV darf das Schutzniveau der DSGVO dabei nicht unterschreiten**.
2. **§ 26 BDSG** regelt auf nationaler Ebene die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses: Beschäftigtendaten dürfen verarbeitet werden, soweit dies für die **Durchführung des Beschäftigungsverhältnisses**

erforderlich ist (§ 26 Abs. 1 Satz 1 BDSG). § 26 Abs. 4 BDSG stellt klar, dass die Verarbeitung auch auf Grundlage von Kollektivvereinbarungen zulässig ist – unter Beachtung von Art. 88 Abs. 2 DSGVO.

3. Unabhängig davon gelten die **allgemeinen DSGVO-Pflichten**: Informationspflichten (Art. 13 DSGVO), Betroffenenrechte (Art. 15 ff. DSGVO), Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) und – bei systematischer Überwachung wie einer GPS-Ortung regelmäßig angezeigt – eine **Datenschutz-Folgenabschätzung** (Art. 35 DSGVO). Binden Sie Ihren Datenschutzbeauftragten frühzeitig ein.

Kurz gesagt: Die BV löst die Mitbestimmungsfrage und kann zugleich die datenschutzrechtliche Grundlage absichern – wenn sie sauber formuliert ist. Genau dafür ist dieses Muster gedacht.

Und ohne Betriebsrat?

Gibt es in Ihrem Betrieb keinen Betriebsrat, entfällt die Mitbestimmungspflicht nach § 87 BetrVG. **Die datenschutzrechtlichen Pflichten bleiben aber vollständig bestehen:** Die Verarbeitung muss auf § 26 Abs. 1 BDSG bzw. Art. 6 Abs. 1 DSGVO gestützt werden, die Beschäftigten müssen vor Inbetriebnahme transparent informiert werden (Art. 13 DSGVO), und die Grundsätze der Zweckbindung und Datenminimierung gelten uneingeschränkt. Vorsicht bei Einwilligungen: Eine Einwilligung im Beschäftigungsverhältnis ist nur unter den engen Voraussetzungen des § 26 Abs. 2 BDSG wirksam (Freiwilligkeit!) und ist als alleinige Grundlage für ein betriebsnotwendiges System meist die falsche Wahl – stützen Sie sich vorrangig auf die Erforderlichkeit nach § 26 Abs. 1 BDSG und schaffen Sie Transparenz. Nutzen Sie dafür den **Alternativ-Baustein „Team-Information“ in Teil 4** dieses Downloads.

Teil 2: Muster-Betriebsvereinbarung

Hinweis: Platzhalter in [eckigen Klammern] sind an Ihren Betrieb anzupassen. Optionale Regelungen sind als solche gekennzeichnet.

Betriebsvereinbarung über die Einführung und Anwendung eines Online-Wächterkontrollsystems

zwischen

der **[Firma, Rechtsform, Anschrift]** – nachfolgend „Arbeitgeber“ –

und

dem **Betriebsrat der [Firma/des Betriebs/Standorts]** – nachfolgend „Betriebsrat“ –

gemeinsam „die Betriebsparteien“.

§ 1 Gegenstand und Geltungsbereich

(1) Diese Betriebsvereinbarung regelt die Einführung, den Betrieb und die Anwendung des Online-Wächterkontrollsystems **[Produktname, z. B. COREDINATE]** – nachfolgend „das System“ – einschließlich der dazugehörigen mobilen Endgeräte, Apps, Kontrollpunkte und des webbasierten Portals.

(2) Sie gilt räumlich für **[den Betrieb/die Betriebe/den Standort ...]** und persönlich für alle Arbeitnehmerinnen und Arbeitnehmer im Sinne des § 5 BetrVG, die das System im Rahmen ihrer Tätigkeit nutzen oder deren Daten durch das System verarbeitet werden. Leitende Angestellte im Sinne des § 5 Abs. 3 BetrVG sind ausgenommen. **[Optional: Auf im Betrieb eingesetzte Leiharbeitnehmer finden die Schutzregelungen dieser Vereinbarung entsprechende Anwendung.]**

(3) Diese Vereinbarung ist zugleich Kollektivvereinbarung im Sinne des Art. 88 Abs. 1 DSGVO i. V. m. § 26 Abs. 4 BDSG. Die Betriebsparteien sind sich einig, dass die hierin geregelte Datenverarbeitung die Anforderungen des Art. 88 Abs. 2 DSGVO wahrt; die Rechte der Beschäftigten aus der DSGVO werden durch diese Vereinbarung nicht eingeschränkt.

§ 2 Zweckbestimmung

(1) Das System wird **ausschließlich** zu folgenden, abschließend aufgezählten Zwecken eingesetzt:

1. **Dienstleistungsnachweis:** Dokumentation der vertragsgemäßen Leistungserbringung (insbesondere Kontrollgänge, Ereignisse, Tätigkeitsnachweise) gegenüber Auftraggebern des Arbeitgebers;

2. **Arbeitssicherheit und Alleinarbeiterschutz:** Schutz der Beschäftigten bei Alleinarbeit und in Gefahrensituationen, insbesondere durch Notruf- und Totmannfunktionen sowie die Lokalisierung im Notfall;
3. **Schichtdokumentation:** Erfassung von Schichtbeginn und Schichtende als Grundlage für Einsatznachweise und die Lohn- und Gehaltsabrechnung;
4. **Organisation des Dienstbetriebs:** Disposition, Objektsteuerung und Qualitätssicherung der Dienstleistung auf Objektebene.

(2) **Eine permanente oder anlasslose Kontrolle des Verhaltens oder der Leistung einzelner Beschäftigter ist ausdrücklich nicht Zweck des Systems und findet nicht statt.** Die durch das System erhobenen Daten dürfen für andere als die in Absatz 1 genannten Zwecke nicht verarbeitet werden; eine Zweckänderung bedarf einer ausdrücklichen Ergänzung dieser Betriebsvereinbarung.

§ 3 Beschreibung des Systems und der erfassten Daten

(1) Das System besteht aus: **[mobile Endgeräte/Smartphones mit App, NFC-/RFID-Kontrollpunkte, webbasiertes Portal, ggf. weitere Komponenten].**

(2) Das System erfasst und verarbeitet folgende Datenarten:

Datenart	Inhalt	Anlass der Erfassung
Scan-Daten	Kontrollpunkt-ID, Datum, Uhrzeit, Objekt/Ort des Kontrollpunkts, scannender Benutzer	Scan eines Kontrollpunkts durch den Beschäftigten
Ereignisdaten	Ereignisart (z. B. Feststellung, Mangel, Vorkommnis), Freitext, ggf. Fotos, Datum, Uhrzeit, Benutzer	Aktive Erfassung durch den Beschäftigten
Schichtdaten	Schichtbeginn, Schichtende, Objekt, Benutzer	An-/Abmeldung zur Schicht
Alarmdaten	Auslösung von Notruf-/Totmannalarm, Zeitpunkt, letzte bekannte Position	Notfall bzw. Alarmauslösung
Positionsdaten (nur bei aktivierter Ortung)	GPS-Position des Dienstgeräts während der laufenden Schicht	Nach Maßgabe von § 4
Stammdaten	Name, Personalnummer, Benutzerkennung, Rolle, zugeordnete Objekte	Einrichtung des Benutzerkontos

(3) **Keine Erfassung außerhalb der Schicht:** Außerhalb einer aktiven Schicht (d. h. vor Schichtbeginn, nach Schichtende und in erfassten Pausen gemäß **[Regelung einfügen]**) erfolgt keine Erfassung von Positions-, Scan- oder Ereignisdaten. Eine Ortung privater Endgeräte findet nicht statt. **[Bei BYOD-Modellen: gesonderte Regelung erforderlich – siehe Ausfüllhilfe, Tipp 8.]**

(4) Das System verfügt über keine Funktionen zur **[z. B. Ton-/Videoaufzeichnung der Beschäftigten, dauerhaften Bewegungsaufzeichnung außerhalb der Schicht]**. Werden solche Funktionen durch Updates verfügbar, gilt § 13.

(5) Eine aktuelle technische Systembeschreibung des Herstellers ist dieser Vereinbarung als **Anlage 1** beigelegt und wird bei wesentlichen Änderungen aktualisiert.

§ 4 GPS-Ortung im Besonderen

(1) Die GPS-Ortung ist **[aktiviert/deaktiviert/nur für folgende Bereiche aktiviert: ...]**. Eine Aktivierung oder Erweiterung der Ortungsfunktion über den hier vereinbarten Umfang hinaus bedarf der vorherigen Zustimmung des Betriebsrats.

(2) Soweit die Ortung aktiviert ist, gilt:

1. Die Position wird **ausschließlich während einer aktiven Schicht** erfasst. Mit Schichtende endet die Positionserfassung automatisch.
2. Die Positionserfassung erfolgt in Intervallen von **[z. B. alle ... Minuten / ereignisbezogen]** und ist batterieschonend ausgestaltet; eine sekundengenaue Dauerverfolgung findet nicht statt.
3. Den Beschäftigten wird der Status der Ortung auf dem Dienstgerät **erkennbar angezeigt** (z. B. durch ein Symbol in der App bzw. die Standortanzeige des Betriebssystems).

4. **Positionsdaten dürfen nicht zur Erstellung von Bewegungsprofilen zum Zweck der Leistungs- oder Verhaltensbewertung einzelner Beschäftigter verwendet werden.** Zulässig bleibt die Nutzung im Rahmen der Zwecke nach § 2 Abs. 1, insbesondere die Lokalisierung im Alarm- und Notfall sowie der objektbezogene Nachweis der Dienstleistung.

5. Im Alarmfall (Notruf, Totmannalarm) darf die aktuelle bzw. letzte bekannte Position abweichend von den Intervallregelungen unmittelbar abgerufen werden, um Hilfe zu leisten.

(3) **[Optional: Außerhalb von Alarmfällen wird die Live-Position nur in aggregierter/objektbezogener Form angezeigt; eine personenbezogene Live-Karte einzelner Beschäftigter steht nur folgendem Personenkreis zur Verfügung: [Rollen].]**

§ 5 Zugriffsrechte und Rollen

(1) Der Zugriff auf die Daten des Systems erfolgt ausschließlich über personengebundene Benutzerkonten mit abgestuften Berechtigungen (Rollenkonzept). Sammelkonten sind unzulässig. Zugriffe werden systemseitig protokolliert.

(2) Es gilt folgendes Rollenkonzept (Einzelheiten in **Anlage 2**):

Rolle	Personenkreis	Zugriff auf
Systemadministration	[z. B. Leitung Einsatzzentrale, max. ... Personen]	Systemkonfiguration, Benutzerverwaltung; Datenzugriff nur soweit erforderlich
Einsatzleitung/Disposition	[Funktionen]	Scan-, Ereignis-, Schicht- und Alarmdaten der zugeordneten Objekte
Objektleitung	[Funktionen]	Daten der eigenen Objekte
Lohnbuchhaltung	[Funktionen]	Schichtdaten (Beginn/Ende) zur Abrechnung
Beschäftigte	alle Nutzer	eigene Erfassungen gemäß § 9

(3) **Auftraggeberzugriff:** Auftraggebern des Arbeitgebers kann ein Lesezugriff (Kunden-/Portalzugang) **ausschließlich auf die mit ihnen vertraglich vereinbarten Objekte** und nur auf objektbezogene Nachweisdaten (Scans, Ereignisse, Berichte) eingeräumt werden. Auftraggeber erhalten **keinen Zugriff** auf Positionsdaten in Echtzeit, auf personenbezogene Auswertungen einzelner Beschäftigter über den Dienstleistungsnachweis hinaus oder auf Daten fremder Objekte. **[Optional: In Objektberichten an Auftraggeber werden Beschäftigte nur mit [Personalnummer/Kürzel] ausgewiesen.]**

(4) Die Liste der Zugriffsberechtigten wird dem Betriebsrat bei Abschluss dieser Vereinbarung und sodann bei jeder Änderung, mindestens jedoch **[halbjährlich]**, zur Verfügung gestellt.

§ 6 Auswertungsverbote und erlaubte Auswertungen

(1) **Erlaubt** sind ausschließlich Auswertungen, die den Zwecken des § 2 Abs. 1 dienen, insbesondere:

1. objektbezogene Auswertungen zum Nachweis der Dienstleistung gegenüber Auftraggebern (z. B. Rundgangsberichte, Ereignisberichte);
2. Auswertungen von Schichtdaten zur Lohn- und Gehaltsabrechnung;
3. **anlassbezogene Auswertungen zur Beweissicherung**, wenn ein konkreter, dokumentierter Anlass vorliegt (z. B. Reklamation eines Auftraggebers, Schadensereignis, behördliche Anfrage, konkreter Verdacht einer schwerwiegenden Pflichtverletzung). Anlassbezogene personenbezogene Auswertungen sind zu dokumentieren; der Betriebsrat wird hierüber **[unverzüglich/innerhalb von ... Tagen]** informiert. **[Optional: Bei Auswertungen wegen des Verdachts einer Pflichtverletzung wird der Betriebsrat vor der Auswertung beteiligt.]**
4. anonymisierte oder aggregierte Auswertungen ohne Personenbezug (z. B. Gesamtzahl Scans pro Objekt) zur Qualitätssicherung.

(2) **Verboten** sind insbesondere:

1. heimliche oder anlasslose Auswertungen des Verhaltens oder der Leistung einzelner Beschäftigter;

2. die Erstellung personenbezogener Leistungsrankings oder Leistungsvergleiche aus Systemdaten;
3. die Auswertung von Positionsdaten zur Bewegungsprofilbildung im Sinne von § 4 Abs. 2 Nr. 4;
4. die Verknüpfung der Systemdaten mit anderen Datenquellen zum Zweck der Verhaltens- oder Leistungskontrolle, soweit nicht in dieser Vereinbarung vorgesehen.

(3) **Verwertungsverbot:** Daten, die unter Verstoß gegen diese Vereinbarung erhoben oder ausgewertet wurden, dürfen nicht zur Begründung personeller Einzelmaßnahmen (insbesondere Abmahnung, Versetzung, Kündigung) oder in Verfahren gegen Beschäftigte verwendet werden. Die Betriebsparteien sind sich einig, dass solche Daten unverzüglich zu löschen sind, soweit keine gesetzliche Aufbewahrungspflicht entgegensteht.

§ 7 Speicherung und Löschung

(1) Personenbezogene Daten des Systems werden nur so lange gespeichert, wie es für die Zwecke nach § 2 Abs. 1 erforderlich ist oder gesetzliche bzw. vertragliche Aufbewahrungspflichten bestehen. Danach werden sie gelöscht oder anonymisiert.

(2) Es gelten folgende Regelfristen:

Datenart	Speicherdauer	Orientierung/Begründung
Scan- und Ereignisdaten	[z. B. ... Monate]	Nachweispflichten gegenüber Auftraggebern gemäß [Vertragslage]; ggf. Verjährungsfristen
Fotos zu Ereignissen	[z. B. ... Monate]	wie vor; frühere Löschung, wenn nicht mehr erforderlich
Schichtdaten	[z. B. ... Jahre]	arbeits-, steuer- und sozialversicherungsrechtliche Aufbewahrungspflichten (u. a. § 257 HGB, § 147 AO, § 17 MiLoG, soweit einschlägig)
Positionsdaten (GPS)	[z. B. ... Tage/Wochen – möglichst kurz]	Alleinarbeiterschutz/Nachweis; keine Langzeitspeicherung erforderlich
Alarmdaten	[z. B. ... Monate]	Dokumentation von Notfällen, Arbeitsschutz
Zugriffsprotokolle	[z. B. ... Monate]	Datensicherheit, Missbrauchskontrolle
Stammdaten	Dauer der Systemnutzung + [Frist]	Benutzerverwaltung

(3) Die Löschung erfolgt **[automatisiert durch das System/durch dokumentierten manuellen Prozess, verantwortlich: [Funktion]]**. Der Arbeitgeber weist dem Betriebsrat auf Verlangen die Umsetzung des Löschkonzepts nach.

(4) Längere Aufbewahrung im Einzelfall ist nur zulässig, soweit Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen in einem konkreten Verfahren benötigt werden; solche Daten sind gesondert zu sperren.

§ 8 Information und Schulung der Beschäftigten

(1) Alle vom System betroffenen Beschäftigten werden **vor der erstmaligen Nutzung** in Textform gemäß Art. 13 DSGVO informiert, insbesondere über: Zwecke, erfasste Daten, Zugriffsberechtigte, Speicherfristen, ihre Rechte nach §§ 9 und 10 sowie die zuständigen Ansprechpartner. Das Informationsblatt ist als **Anlage 3** beigelegt.

(2) Die Beschäftigten erhalten vor dem Einsatz eine angemessene Einweisung in die Bedienung des Systems (einschließlich Notruf- und Totmannfunktionen) während der Arbeitszeit. Die Teilnahme gilt als Arbeitszeit.

(3) Neue Beschäftigte werden im Rahmen des Onboardings entsprechend informiert und geschult.

(4) Diese Betriebsvereinbarung wird allen Beschäftigten in geeigneter Weise zugänglich gemacht **[z. B. Aushang, Intranet, Aushändigung]**.

§ 9 Rechte der Beschäftigten

(1) Die Rechte der Beschäftigten aus der DSGVO – insbesondere Auskunft (Art. 15), Berichtigung (Art. 16), Löschung (Art. 17) und Einschränkung der Verarbeitung (Art. 18) – bleiben unberührt.

(2) Beschäftigte haben das Recht, auf Antrag **Einsicht in die über sie im System gespeicherten Daten** zu erhalten, insbesondere in ihre Scan-, Schicht- und – soweit erfasst – Positionsdaten. Die Einsicht wird innerhalb von **[z. B. zwei Wochen]** gewährt; auf Wunsch kann ein Mitglied des Betriebsrats hinzugezogen werden.

(3) Anträge sind zu richten an: **[Funktion/Stelle, Kontakt]**. Der/die Datenschutzbeauftragte ist erreichbar unter: **[Kontakt]**.

(4) Beschäftigten entstehen aus der Wahrnehmung ihrer Rechte nach dieser Vereinbarung keine Nachteile.

§ 10 Keine Sanktionen aufgrund reiner Systemdaten ohne Anhörung

(1) Personelle Einzelmaßnahmen (insbesondere Ermahnung, Abmahnung, Versetzung, Kündigung) dürfen **nicht allein auf Daten des Systems gestützt** werden.

(2) Vor jeder personellen Maßnahme, bei der Systemdaten herangezogen werden sollen, ist der/dem betroffenen Beschäftigten **Gelegenheit zur Stellungnahme** zu den Daten und ihrem Zustandekommen zu geben. Dabei ist insbesondere zu berücksichtigen, dass Systemdaten unvollständig oder technisch bedingt fehlerhaft sein können (z. B. defekter Kontrollpunkt, fehlender GPS-/Netzeempfang, Geräteausfall, Akkustand).

(3) Auf Wunsch der/des Beschäftigten kann zu der Anhörung ein Mitglied des Betriebsrats hinzugezogen werden. Die Beteiligungsrechte des Betriebsrats (insbesondere §§ 99, 102 BetrVG) bleiben unberührt.

§ 11 Rechte des Betriebsrats

(1) Der Betriebsrat erhält **[einen lesenden Zugang zum System mit folgendem Umfang: .../auf Verlangen Einsicht in die Systemkonfiguration, das Rollenkonzept und die Auswertungsfunktionen]**, soweit dies zur Überwachung der Einhaltung dieser Vereinbarung erforderlich ist. Personenbezogene Daten einzelner Beschäftigter sieht der Betriebsrat dabei nur, soweit dies zur Aufgabenwahrnehmung erforderlich ist.

(2) Der Betriebsrat ist berechtigt, **[einmal jährlich/anlassbezogen]** gemeinsam mit dem Arbeitgeber ein **Audit** durchzuführen, das insbesondere umfasst: Rollenkonzept und Zugriffsberechtigungen, durchgeführte anlassbezogene Auswertungen nach § 6 Abs. 1 Nr. 3, Umsetzung des Löschkonzepts nach § 7 sowie zwischenzeitliche Systemänderungen.

(3) Der Betriebsrat kann zur Beurteilung des Systems nach Maßgabe des § 80 Abs. 3 BetrVG **Sachverständige hinzuziehen**; die Einzelheiten (Person, Kosten) werden zwischen den Betriebsparteien vereinbart. Sein Recht, den/die Datenschutzbeauftragte/n zu konsultieren, bleibt unberührt.

(4) Der Arbeitgeber informiert den Betriebsrat rechtzeitig und umfassend über geplante Änderungen im Sinne des § 13 sowie über meldepflichtige Datenschutzvorfälle mit Bezug zum System.

§ 12 Testbetrieb / Pilotphase

(1) Das System wird zunächst für die Dauer von **[z. B. drei Monaten]** in einem Pilotbetrieb eingeführt. Der Pilotbetrieb umfasst **[Objekte/Bereiche/Anzahl Beschäftigte]**.

(2) Während des Pilotbetriebs gelten sämtliche Schutzregelungen dieser Vereinbarung uneingeschränkt. **Daten aus dem Pilotbetrieb dürfen nicht für personelle Einzelmaßnahmen verwendet werden.**

(3) Nach Abschluss des Pilotbetriebs werten die Betriebsparteien die Erfahrungen **gemeinsam** aus (u. a. Praxistauglichkeit, Akzeptanz, technische Zuverlässigkeit, Erfüllung der Zweckbindung). Über Anpassungen dieser Vereinbarung wird auf dieser Grundlage verhandelt. **[Optional: Kommt keine Einigung über die Fortführung zustande, gilt .../entscheidet die Einigungsstelle.]**

(4) Die Beschäftigten des Pilotbereichs werden über Beginn, Umfang und Ende des Pilotbetriebs gesondert informiert und erhalten Gelegenheit zu Rückmeldungen an **[Stelle]** und an den Betriebsrat.

§ 13 Änderungen des Systems (Update-Klausel)

(1) **Unwesentliche Änderungen** (insbesondere Fehlerbehebungen, Sicherheitsupdates, Änderungen der Benutzeroberfläche ohne neue Datenerfassung oder Auswertungsmöglichkeiten) kann der Arbeitgeber ohne gesonderte Beteiligung umsetzen. Der Betriebsrat wird über solche Updates **[regelmäßig/quartalsweise]** in zusammengefasster Form informiert.

(2) **Wesentliche Änderungen** – insbesondere die Erfassung neuer Datenarten, neue oder erweiterte Auswertungs- und Ortungsfunktionen, geänderte Zugriffskonzepte oder die Aktivierung bislang deaktivierter Funktionen – dürfen erst nach vorheriger Information des Betriebsrats und Einigung der Betriebsparteien produktiv genutzt werden. Bis zur Einigung bleiben solche Funktionen deaktiviert.

(3) Stellt der Hersteller Funktionen standardmäßig bereit, die nach dieser Vereinbarung nicht genutzt werden dürfen, stellt der Arbeitgeber durch Konfiguration sicher, dass sie deaktiviert bleiben, und dokumentiert dies auf Verlangen gegenüber dem Betriebsrat.

(4) Anlage 1 (Systembeschreibung) wird bei wesentlichen Änderungen fortgeschrieben.

§ 14 Schlussbestimmungen

(1) Diese Betriebsvereinbarung tritt am **[Datum]** in Kraft.

(2) Sie kann mit einer Frist von **[z. B. drei Monaten zum Quartalsende]** schriftlich gekündigt werden. **[Variante A: Sie wirkt in den Angelegenheiten der zwingenden Mitbestimmung nach § 87 BetrVG gemäß § 77 Abs. 6 BetrVG nach, bis sie durch eine andere Abmachung ersetzt wird.] [Variante B: Eine Nachwirkung wird ausgeschlossen; mit Ablauf der Kündigungsfrist ist der Betrieb des Systems einzustellen, bis eine neue Vereinbarung geschlossen ist.]**

(3) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

(4) **Salvatorische Klausel:** Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Betriebsparteien verpflichten sich, eine unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem verfolgten Zweck am nächsten kommt.

(5) Bei Meinungsverschiedenheiten über die Auslegung oder Anwendung dieser Vereinbarung bemühen sich die Betriebsparteien zunächst um eine einvernehmliche Lösung. **[Optional: Kommt eine Einigung nicht zustande, entscheidet die Einigungsstelle gemäß § 76 BetrVG.]**

Anlagen:

- Anlage 1: Technische Systembeschreibung
- Anlage 2: Rollen- und Berechtigungskonzept
- Anlage 3: Informationsblatt für Beschäftigte (Art. 13 DSGVO)

[Ort], den [Datum]

[Geschäftsführung]

[Betriebsratsvorsitzende/r]

Teil 3: Ausfüllhilfe – die erfahrungsgemäß strittigen Punkte und wie Sie sie lösen

Tipp 1 – Zweckbindung eng fassen schafft Vertrauen (§ 2). Der häufigste Fehler von Arbeitgeberseite: Zwecke bewusst weit oder „auf Vorrat“ formulieren („...und sonstige betriebliche Zwecke“). Das wirkt auf Betriebsräte wie eine Hintertür und blockiert Verhandlungen. Eine **abschließende, enge Zweckliste** kostet Sie in der Praxis nichts – Dienstleistungsnachweis, Arbeitsschutz und Abrechnung decken den realen Bedarf ab – und ist das stärkste Vertrauenssignal, das Sie senden können.

Tipp 2 – Den Alleinarbeiterschutz als Fürsorge-Argument führen (§ 2, § 4). Notruf- und Totmannfunktion sind keine Überwachung, sondern gelebte Fürsorgepflicht: Bei Alleinarbeit nachts im Objekt kann die Lokalisierung im Notfall Leben retten (vgl. die Anforderungen an die Organisation von Alleinarbeit nach DGUV-Regelwerk). Stellen Sie diesen Punkt an den Anfang des Gesprächs mit dem Betriebsrat – er verschiebt die Wahrnehmung des Systems von „Kontrolle“ zu „Schutz“.

Tipp 3 – GPS ist der emotionalste Punkt: Differenzieren statt pauschal fordern (§ 4). „Ortung ja/nein“ als Alles-oder-nichts-Frage führt in die Blockade. Verhandeln Sie stattdessen die Stellschrauben einzeln: nur während der Schicht (technisch ohnehin so vorgesehen), Erfassungsintervall, wer die Position sieht, Live-Ansicht nur im Alarmfall, kurze

Löschfrist für Positionsdaten. Oft ist eine Lösung konsensfähig, bei der GPS primär dem Notfall dient und für Routine-Auswertungen gar nicht zur Verfügung steht.

Tipp 4 – Das Auswertungsverbot ist das Herzstück für den Betriebsrat (§ 6). Die Sorge ist fast nie das Scannen selbst, sondern die heimliche Einzelauswertung („Wer war am langsamsten?“). Die Kombination aus anlassloser-Auswertung-verboten + anlassbezogene Beweissicherung dokumentiert und BR-informiert + Verwertungsverbot bei Verstößen löst diesen Knoten in den meisten Verhandlungen. Bestehen Sie als Arbeitgeber aber auf der **anlassbezogenen Beweissicherung bei Reklamationen** – ohne sie verliert das System seinen Hauptnutzen als Nachweisinstrument.

Tipp 5 – Pilotphase mit gemeinsamer Auswertung anbieten (§ 12). Wenn der Betriebsrat zögert: Eine befristete Pilotphase mit ausdrücklichem Sanktionsverbot und gemeinsamer Auswertung senkt die Einstiegshürde enorm. Beide Seiten verhandeln dann über ein System, das sie aus der Praxis kennen – nicht über Befürchtungen. Planen Sie die Auswertungssitzung von Anfang an mit festem Termin ein.

Tipp 6 – Löschfristen: kurz bei GPS, lang nur wo Pflichten bestehen (§ 7). Strittig sind fast immer die Positionsdaten. Faustregel, die Verhandlungen entschärft: **Positionsdaten so kurz wie möglich** (Tage bis wenige Wochen), Scan-/Ereignisdaten orientiert an den vertraglichen Nachweispflichten gegenüber Auftraggebern, Schichtdaten entlang der gesetzlichen Aufbewahrungspflichten. Wer für jede Datenart eine Begründung in die Tabelle schreibt, nimmt der Fristen-Diskussion die Beliebigkeit. Stimmen Sie die Fristen mit Ihrem Datenschutzbeauftragten ab.

Tipp 7 – Auftraggeberzugriff transparent machen (§ 5 Abs. 3). Betriebsräte reagieren empfindlich, wenn „der Kunde unsere Leute überwachen kann“. Die Lösung: Kundenzugriff strikt objektbezogen, keine Echtzeit-Position für Auftraggeber, optional Pseudonymisierung in Kundenberichten (Personalnummer statt Klarname). Das ist für Auftraggeber in aller Regel völlig ausreichend – sie wollen den Nachweis der Leistung, nicht die Person.

Tipp 8 – Dienstgeräte statt BYOD. Die saubere Lösung sind arbeitgebereigene Dienstgeräte: klare Trennung von privat und dienstlich, keine Diskussion über Ortung privater Handys, einfachere Konfiguration. Wenn Sie private Geräte einsetzen wollen (BYOD), regeln Sie zwingend gesondert: keine Erfassung außerhalb der App/Schicht, Freiwilligkeit, Kostenerstattung – und rechnen Sie mit deutlich längeren Verhandlungen.

Tipp 9 – Update-Klausel früh ansprechen (§ 13). Cloud-Software ändert sich laufend. Ohne Update-Klausel müsste streng genommen jedes Feature-Update neu mitbestimmt werden – das will keine Seite. Die Trennung „unwesentlich = Information“ / „wesentlich (neue Daten, neue Auswertungen) = Einigung vor Aktivierung“ ist der etablierte Kompromiss und erspart beiden Seiten Dauerkonflikte.

Tipp 10 – Anhörungsrecht vor Sanktionen großzügig zusagen (§ 10). Dass niemand allein wegen eines „fehlenden Scans“ abgemahnt wird, sollte für Sie als Arbeitgeber selbstverständlich sein – Systemdaten können schlicht falsch sein (defekter Tag, kein Empfang, leerer Akku). Diese Zusage kostet nichts, ist gelebte Fairness und ist regelmäßig der Punkt, an dem die Belegschaft kippt: vom Misstrauen zur Akzeptanz.

Teil 4: Alternativ-Baustein für Betriebe OHNE Betriebsrat – „Team-Information zur Einführung“

Diesen einseitigen Text können Sie als Aushang, Anlage zur Lohnabrechnung oder im Team-Meeting verwenden. Er ersetzt nicht die förmliche Datenschutzinformation nach Art. 13 DSGVO, kann aber mit dieser kombiniert werden. Platzhalter anpassen.

Team-Information: Einführung unseres digitalen Wächterkontrollsystems

Liebe Kolleginnen und Kollegen,

ab dem **[Datum]** setzen wir das digitale Wächterkontrollsystem **[Produktname, z. B. COREDINATE]** ein. Hier steht transparent, was das für euch bedeutet.

Warum führen wir das System ein?

1. Um unseren Auftraggebern nachzuweisen, dass unsere Arbeit zuverlässig erledigt wurde – das sichert Aufträge und damit Arbeitsplätze.

2. Für eure **Sicherheit**: Notruf- und Totmannfunktion sorgen dafür, dass im Ernstfall – gerade bei Alleinarbeit nachts – schnell Hilfe kommt.
3. Für eine korrekte und einfache **Schicht- und Lohnabrechnung**.

Was wird erfasst?

- Scans der Kontrollpunkte (welcher Punkt, wann)
- Ereignismeldungen, die ihr aktiv erfasst (Text, ggf. Fotos)
- Schichtbeginn und Schichtende
- **[Falls aktiviert:]** die GPS-Position des Dienstgeräts – **nur während eurer Schicht**, primär für den Notfall

Was wird NICHT erfasst und NICHT gemacht?

- Keine Erfassung außerhalb eurer Schicht und keine Ortung privater Handys
- Keine permanente Kontrolle eures Verhaltens oder eurer Leistung
- Keine heimlichen Einzelauswertungen und keine Leistungsrankings
- Niemand wird allein aufgrund von Systemdaten abgemahnt – ihr werdet immer zuerst angehört

Wer sieht die Daten? Nur Berechtigte mit eigenem Zugang: **[z. B. Einsatzleitung, Objektleitung, Lohnbuchhaltung]** – jeweils nur, was sie für ihre Aufgabe brauchen. Auftraggeber sehen ausschließlich die Nachweise für ihr eigenes Objekt, keine Echtzeit-Position.

Wie lange werden Daten gespeichert? Nur so lange wie nötig: **[Kurzfassung der Fristen, z. B. „Positionsdaten ... Tage, Nachweisdaten ... Monate, Schichtdaten nach gesetzlichen Vorgaben“]** – danach werden sie gelöscht.

Eure Rechte: Ihr könnt jederzeit Auskunft über eure gespeicherten Daten verlangen und sie einsehen (Art. 15 DSGVO), Berichtigung und ggf. Löschung verlangen. Eine ausführliche Datenschutzhinweise erhaltet ihr **[mit dieser Information/im Anhang]**.

Eure Ansprechpartner: Fragen zum System: **[Name, Funktion, Kontakt]** · Datenschutz: **[Name/Stelle des Datenschutzbeauftragten, Kontakt]**

Wir führen das System offen und fair ein. Wenn euch etwas unklar ist oder stört: Sprecht uns an – vor dem Start gibt es eine Einweisung für alle.

[Geschäftsführung, Datum, Unterschrift]

Teil 5: Disclaimer

Dieses Dokument ist ein **unverbindliches Muster** und dient ausschließlich der allgemeinen Information und als Arbeitsgrundlage. Es ersetzt **keine Rechtsberatung** im Einzelfall. Betriebsvereinbarungen müssen stets auf die konkreten betrieblichen Verhältnisse, die eingesetzte Systemkonfiguration, die einschlägigen Tarifverträge und den aktuellen Stand von Gesetzgebung und Rechtsprechung angepasst werden. Lassen Sie die finale Fassung **vor Abschluss durch eine Fachanwältin/einen Fachanwalt für Arbeitsrecht und Ihre/n Datenschutzbeauftragte/n prüfen**. Die COREDINATE GmbH übernimmt keine Haftung für die Verwendung dieses Musters.

Stand: Juni 2026 · Herausgeber: COREDINATE GmbH, Ringstraße 25, 97215 Uffenheim, www.coredinate.de