



Dr. Eberhard Kiesche

Checkliste: Tipps aus der Beratungspraxis zur Abfassung von IT-/ Beschäftigtendatenschutz-Betriebsvereinbarungen (Stand 02.12.2022)

Die folgende Checkliste enthält Tipps, worauf Betriebsräte/Personalräte achten sollen, wenn sie Betriebsvereinbarungen zu technischen Kontrolleinrichtungen und zum Beschäftigtendatenschutz gemäß § 87 Abs. 1 Nr. 1, 6 BetrVG (z.B. IT-gestützte Zeiterfassung, Einführung und Anwendung von dienstlichen Smartphones, IuK-Rahmenbetriebsvereinbarung, E-Mail und Internet, Videoüberwachung, Torkontrollen), § 26 Abs. 4 BDSG und Art. 88 Abs. 1, 2 DSGVO (EU-Datenschutz-Grundverordnung) entwickeln und abschließen wollen.

1. Der **Titel der Betriebsvereinbarung und der sachliche Geltungsbereich** sind so zu formulieren, dass der sachliche Gegenstand bzw. Geltungsbereich der Betriebsvereinbarung zutreffend umfassend bezeichnet wird: „Einführung, Anwendung, Änderung, Weiterentwicklung, Außerbetriebnahme ...“.

Der *personelle Geltungsbereich* sollte sich auf auch Bewerber beziehen, da diese im datenschutzrechtlichen Begriff des Beschäftigten aufgenommen sind (§ 26 Abs. 8 BDSG). Für leitende Angestellte sollte der Arbeitgeber sich verpflichten, die vereinbarten Regelungen ebenso umzusetzen, z. B. durch Einwilligungen.

2. In der **Präambel**, die kurz zu halten ist, sollten die Interessen der Arbeitgeber und der Arbeitnehmer für die Interessenabwägung mindestens *gleichwertig* formuliert sein. Der **Persönlichkeitsschutz der Beschäftigten, die informationelle Selbstbestimmung und das Recht auf Datenschutz** (u.a. Art. 8 Grundrechtecharta - GRCh) sind aufzuführen, ebenso die maximale Wahrung und Förderung der Rechte des Betriebs- bzw. Personalrats und der Beschäftigten als datenschutzrechtlich Betroffene (siehe Art. 88 Abs. 2 DSGVO).

3. Die datenschutzkonforme **Verarbeitung von personenbezogenen Daten der Beschäftigten** insbesondere bei der Regelung aller technischen Kontrolleinrichtungen muss als sachlicher Gegenstandsbereich gleichwertig aufgenommen werden. Dabei sollte insbesondere die Regelungsinhalte § 26 BDSG berücksichtigt werden. Zusätzlich sind in der Betriebsvereinbarung *die Zwecke*, die mit der Datenverarbeitung und der technischen Kontrolleinrichtung verfolgt werden, *so eng wie möglich, eindeutig, konkret und verständlich* festzulegen (Art. 5 Abs. 1 lit. b DSGVO). Dadurch wird die abschließende **Zweckbindung** geregelt und mögliche Zweckänderungen ausgeschlossen bzw. erschwert. Zweckänderungen (z.B. nach Art. 6 Abs. 4 DSGVO) sind zu untersagen bzw. nach der DSGVO zu erschweren. Zwecke für die Datenerhebung dürfen keinesfalls in einer IT-Rahmenbetriebsvereinbarung *auf Vorrat* oder zu vage bzw. zu allgemein vom Betriebsrat genehmigt werden.



4. Es ist strikt **Bezug auf die gesetzliche Begriffsbestimmungen** (sogenannte Legaldefinitionen), soweit vorhanden, im geltenden Datenschutzrecht (siehe Art 4 DSGVO, § 2 BDSG) zu nehmen. Betriebsräte bzw. Betriebsparteien sollten unbedingt auf eine immer fehlerhafte Umformulierung in eigenen Worten verzichten. Ein Beispiel dafür ist „Beschäftigungsdaten“ statt „personenbezogene Daten der Beschäftigten“.

Im Bereich des Betriebsverfassungsrechts müssen eindeutig definierte Begriffe genutzt werden, so z.B. Mitbestimmung statt Benehmen, Mitwirkung oder Beteiligung.

Sind es Begriffe, die (noch) nicht rechtlich (legal) definiert sind, **empfehlen sich Definitionen bzw. Erläuterungen, z. B. in einem gesonderten Anhang (Glossar)**.

5. **Unbestimmte Rechtsbegriffe** wie z.B. angemessen, erforderlich, rechtzeitig, umfassend, grundsätzlich oder *verhältnismäßig* lassen sich nicht vermeiden. Dann sind sie jedoch möglichst mit sprechenden Beispielen bzw. Verweisen auf Rechtsquellen rechtsklar zu definieren bzw. anschaulich zu erläutern.

6. In Betriebsvereinbarungen zu technischen Kontrolleinrichtungen bzw. Überwachungssystemen am Arbeitsplatz muss stets eine **sorgfältige Dokumentation** des einzuführenden Systems bzw. der Technologie vereinbart werden, damit die Transparenz nach Art. 5 Abs. 1 lit. a DSGVO für die Beschäftigten und für die Interessenvertretungen gewahrt bleibt bzw. hergestellt wird. Die bloße Übernahme eines Glossars oder einer Beschreibung des Herstellers sind unzureichend. Die **abschließende, klare und verständliche Dokumentation** von Hard- und Software, Zwecke, Vernetzung, Art und Umfang der Daten (Datenkatalog) und zulässige Auswertungen, Empfänger der Daten, *Schnittstellen*, Speicherbegrenzungsfristen/Löschkonzepte und Zugriffsberechtigungen dient dem Betriebsrat dazu, den *Ist-Zustand des Systems* festzuschreiben und abschließend zu regeln. Nur so kann er eine Kontrolle ausüben, ob die Betriebsvereinbarung eingehalten wird. Damit wird der Transparenzpflicht des Arbeitgebers nach DSGVO (Art. 5 Abs. 1 lit. a) genüge getan.

Betriebsräte können dann während der Anwendung des Systems überprüfen, inwieweit Änderungen und Erweiterungen des Systems durch die Interessenvertretung geregelt bzw. mitbestimmt worden sind. Die Dokumentation dient auch dazu, die Anforderungen des BDSG und der DSGVO zu erfüllen, damit die abzuschließende Betriebsvereinbarung als *vorrangige Rechtsvorschrift* nach § 26 Abs. 4 BDSG / Art. 6, 88 Abs. 1 und 2 DSGVO herangezogen werden kann. Sie dient, so für die zuständige Aufsichtsbehörde für den Datenschutz, zum *Nachweis, dass die DSGVO eingehalten wird* (Art. 5 Abs. 2 DSGVO).



7. **Systematisch aufgebaute Betriebsvereinbarungen zum Beschäftigtendatenschutz** müssen *rechtsklare Verbote, Gebote, grundlegende Sachverhalte und vor allem konkrete Prinzipien des Datenschutzes und Begriffsbestimmungen* enthalten. So müssen in Betriebsvereinbarungen zu technischen Kontrolleinrichtungen u.a. ein klares und eindeutiges *Verbot von Leistungs- und Verhaltenskontrollen*, ein ausreichend formuliertes *Beweisverwertungsverbot* und ein **Nachteilsverbot** (*Maßregelungsverbot* § 612a BGB) geregelt werden. Die *Rechtsfolgen* bei Missbrauch und Verstößen gegen die Betriebsvereinbarung durch den Arbeitgeber (z. B. bei heimlichen oder unzulässigen Kontrollen) sind festzuhalten.

8. **Betriebsvereinbarungen (Kollektivvereinbarungen – siehe Art. 88 Abs. 1 DSGVO und ErwGr 155)** müssen, wenn sie als vorrangige Rechtsvorschriften zur Rechtfertigung der Verarbeitung von Beschäftigtendaten gelten sollen, *konkret, transparent und rechtsklar* die technische Kontrolleinrichtung regeln. Das bedeutet, dass z. B. personenbezogene Beschäftigtendaten, die verarbeitet werden dürfen, in einer *Positivliste erfasst sind und damit Art und Umfang der verarbeiteten Daten ersichtlich* werden. Diese Daten dürfen verarbeitet werden, alle anderen Daten sind verboten.

Ebenso müssen Auswertungen, Zwecke und Zweckbindung, Löschfristen, Maßnahmen zur Datenminimierung, Schnittstellen zu anderen IT-Verfahren, Zugriffsrechte, Empfänger der Daten sowie technische und organisatorische Datenschutzmaßnahmen so bestimmt und konkret wie möglich festgelegt werden.

Wichtige Informationen für diese grundlegenden Inhalte von Einzelbetriebsvereinbarungen zu technischen Kontrolleinrichtungen können dem *Verzeichnis von Verarbeitungstätigkeiten* (VVT - Art. 30 DSGVO) entnommen werden, wenn es umfassend mit wichtigen Ergänzungen erstellt und vom Datenschutzbeauftragten *aktuell* geführt wird. Der Betriebsrat hat **nach § 80 Abs. 1 Nr. 1 und Abs. 2 BetrVG** auf das VVT einen Informationsanspruch und kann die Herausgabe des aktuellen Verzeichnisses verlangen.

Vorausgesetzt ist für die Prüfung von Verarbeitungstätigkeiten stets eine Vorab-Prüfung der datenschutzrechtlichen Zulässigkeit bzw. der Rechtmäßigkeit (siehe Art. 5 Abs. 1 lit. a DSGVO). In Fällen der Einführung von technischen Systemen oder Software mit Verarbeitung von (schützenswerten sensiblen) Beschäftigtendaten ist in der Regel auch eine *Datenschutzfolgenabschätzung* nach Art. 35, 36 DSGVO erforderlich. Oftmals werden Gesundheitsdaten personalaktenrechtlich nicht korrekt aufbewahrt oder das erforderliche Vorgehen für *Datentransfers in Drittstaaten* gewählt. Auch *Datenflüsse im Konzern* sind normgerecht in Betriebsvereinbarungen zu gestalten und bereiten in der Praxis den Betriebsparteien oftmals Schwierigkeiten. Bei offenen Streitfragen kann bzw. sollte die jeweilige Aufsichtsbehörde für den Datenschutz auch vom Betriebsrat eingeschaltet werden. Vorher ist aber in der Regel nach dem BAG intern eine Klärung zu versuchen.



Inhalte von Betriebsvereinbarungen zum Beschäftigtendatenschutz

- Ziele der BV und Regelungsgegenstand
- Zwecke der Kontrolleinrichtung, Zweckbindung
- Geltungsbereich
- Systembeschreibung: Hard- und Software, Daten- und Auswertungskatalog, Schnittstellen, Berechtigungen
- Begriffsbestimmungen
- Art und Umfang der Daten
- Ausschluss von Leistungs- und Verhaltenskontrollen
- Ggf. Regelungen zur Auftragsverarbeitung nach Art. 28 DSGVO und Rechte des Betriebsrats
- Rechte der betroffenen Beschäftigten nach Art. 12 ff. DSGVO, Schutzbestimmungen nach Art. 88 Abs. 2 DSGVO
- Rechte des Betriebsrates (Informations- und Mitbestimmungsrechte und -verfahren, Überwachungsrechte, erforderliche Zugriffsrechte auf personenbezogene Daten einschließlich Systemaudit mit Sachverständigen, ggf. Online-Zugriffe)
- Empfänger der Daten
- Technische und organisatorische Maßnahmen des Datenschutzes, z.B. Berechtigungskonzept, Verschlüsselung, Protokollierung
- Konkrete Lösch- bzw. Speicherfristen (bzw. Löschkonzept)
- Verfahren bei Streitigkeiten
- Schlussbestimmungen, Kündigung und Nachwirkung.

Ebenso ist zusätzlich das **Verfahren zur Mitbestimmung der Interessenvertretung** zur datenschutzrechtlichen Prüfung der Zulässigkeit der Datenverarbeitung zu regeln. Dabei dürfen gesetzliche Rechte der Betriebsräte *auf keinen Fall unterschritten* werden.

9. Deklaratorische Verweise auf gesetzliche Grundlagen des Datenschutzes oder der Betriebsverfassung können entgegen der Meinung von Arbeitgebern und deren Anwälte durchaus eingesetzt werden, allerdings sparsam und richtig zu Zwecke der Transparenz, Information und der Schulung. Es erleichtert auch die Wahrnehmung z.B. des Rechts auf Schadensersatz nach Art. 82 DSGVO. Das verdeutlicht rechtsklar den Arbeitgebern bzw. den Führungskräften ihre rechtlichen Pflichten, die sie einzuhalten haben (im Sinne von DSGVO-Compliance: Befolgen von Rechtsvorschriften und Unternehmensregeln) und den Beschäftigten und Interessenvertretungen ihre gesetzlichen Rechte.

Für Betriebsräte ist jedoch wichtiger, dass im Text der Betriebsvereinbarung eine **weitgehende betriebliche Konkretisierung z.B. der gesetzlichen Datenschutzprinzipien und Mitbestimmungsregeln** erfolgt, d.h. die konkrete Umsetzung des Arbeits- und Datenschutzrechts im Beschäftigungsverhältnis ist zu regeln. Hierfür eröffnen sich betriebliche Ermessensspielräume. Dafür sind konkretisierende Verweise auf die



gesetzlichen Grundlagen des Datenschutzrechts, z.B. auf § 75 Abs. 1 und 2 BetrVG, erforderlich.

10. **Leerformeln und Selbstverständlichkeiten** sind zu vermeiden: „Die Einhaltung der Regelungen des BDSG wird beachtet.“ „Es besteht Einigkeit, dass ...“ „Der Arbeitgeber sichert zu, dass ...“ „Der Arbeitgeber stellt fest, dass ...“

11. **Aufzählungen sind abschließend zu formulieren**, wenn keine Ausnahmen zugelassen werden sollen. Die Worte „insbesondere, u.a. und zum Beispiel“ öffnen die Aufzählung für weitere, dann zulässige Tatbestände.

12. Für jeden Abschnitt der Betriebsvereinbarung ist eine **aussagekräftige Überschrift** zu wählen. In jedem Abschnitt der Vereinbarung ist sachlich immer *nur ein Thema bzw. dessen Unterpunkte* zu regeln. Dabei bietet es sich an, in der Betriebsvereinbarung eine *bestimmte Reihenfolge der Absätze und der Sätze in einem Abschnitt einzuhalten*. Die Betriebsvereinbarung als Rechtsvorschrift ist wie ein Gesetz aufzubauen, mit Paragrafen, klaren Absätzen und Sätzen. Das erleichtert die konkreten Verhandlungen mit dem Arbeitgeber bzw. seinen Juristen zw. die Arbeit in Einigungsstellen.

13. In IT-Betriebsvereinbarungen ist allerdings ein **Beweisverwertungsverbot** in einem gesonderten Abschnitt mit der richtigen Überschrift rechtssicher zu regeln, oftmals auch ein Nachteilsverbot. Es fehlt bislang ein gesetzliches Beweisverwertungsverbot. Die Rechtsprechung des Bundesarbeitsgerichts (BAG) ist in dieser Frage uneinheitlich und besonders schwierig, so dass der betroffene Arbeitnehmer und die Betriebsräte ohne einem Beweisverwertungsverbot in der Betriebsvereinbarung vor Gericht in Schwierigkeiten geraten. Vor Gericht und/oder in Einigungsstellen kann ein Beweisverwertungsverbot trotzdem scheitern. Es gibt aber auch Arbeitgeber, die mit der Aufnahme eines Beweisverwertungsverbot in der Betriebsvereinbarung einverstanden sind.

14. Ein bloßer Hinweis auf die gesetzlichen Aufbewahrungsfristen (Speicherbegrenzungsfristen nach Art. 5 Abs. 1 lit. e DSGVO) von personenbezogenen Daten genügt in der Vereinbarung grundsätzlich nicht, weil daraus keine tatsächliche Löschung der personenbezogenen Daten erfolgt, wenn diese nicht mehr nach Art. 17 Abs. 1 lit. a DSGVO erforderlich sind. Es müssen **konkrete Lösungs- und Aufbewahrungsfristen** für die Beschäftigtendaten in die Vereinbarung aufgenommen werden, z.B. in Form einer Anlage, deren Einhaltung vom Betriebsrat überprüft werden kann. Ggf. kann – wenn dies nicht möglich ist - ein Konzept zur Löschung bzw. Begrenzung der Speicherdauer vereinbart werden.

15. In **den BV-Schlussbestimmungen** sind mindestens das Inkrafttreten, die Kündigungsfristen und die **salvatorische Klausel** zu regeln. Die Nachwirkung muss in jedem Einzelfall von der Interessenvertretung sorgfältig überlegt werden, je nachdem, wie der Betriebsrat in den Verhandlungen mit dem Arbeitgeber seine Ziele, Eckpunkte, KO-Kriterien und Forderungen durchsetzen konnte.



16. In jedem Einzelfall ist mit **Anlagen zur Betriebsvereinbarung** zu arbeiten, da diese einfacher zu ändern sind. Vor dem Inkrafttreten der Betriebsvereinbarung müssen immer sämtliche Anlagen erstellt, vereinbart und unterzeichnet sein.

17. Die Betriebsvereinbarung muss den Anforderungen der DSGVO und des BDSG entsprechen. **Der Schutzstandard darf keinesfalls unterschritten werden**, wie manche Arbeitgeberjuristen immer noch behaupten. Die besonderen Maßnahmen zum Schutz der Menschenwürde, Rechte und Freiheiten der Beschäftigten nach Art. 88 Abs. 2 DSGVO dürfen allerdings **zu Gunsten der Beschäftigten verbessert** werden. Altbetriebsvereinbarungen mit datenschutzrechtlicher Relevanz sind anzupassen, ansonsten verstoßen sie gegebenenfalls gegen höherrangiges Recht und werden unanwendbar, zumindest mit einzelnen Bestimmungen.