



ZAAR

Zentrum für Arbeitsbeziehungen
und Arbeitsrecht

VORTRAGSREIHE

Donnerstag, 17. September 2026 / 19:00 Uhr

Betriebsrat und Beschäftigtendatenschutz

Referent:

Dr. Philipp Byers

Dentons Europe (Germany) GmbH & Co. KG

Agenda

I. Reichweite der erzwingbaren Mitbestimmungsrechte beim Beschäftigtendatenschutz

II. Gestaltungsmöglichkeiten einer Betriebsvereinbarung als datenschutzrechtliche Erlaubnisnorm

III. Datenschutzrechtliche Pflichten des Betriebsrats nach § 79a BetrVG

IV. Beteiligungsrechte des Betriebsrats vs. Persönlichkeitsschutz der Mitarbeiter: Wo liegen die rechtlichen Grenzen?

I. Reichweite der erzwingbaren Mitbestimmung

1. Rechtliche Grundlagen

- In Betrieben mit Betriebsrat sind beim Umgang mit Beschäftigtendaten oftmals Mitbestimmungsrechte des Betriebsrats zu beachten.
- Regelmäßig ist das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG („**technische Überwachung**“ aufgrund des weiten Überwachungsbegriffs bei der Verarbeitung von Mitarbeiterdaten relevant.
- Bei „analogen“ Kontrollen am Arbeitsplatz kann auch das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 1 BetrVG („**Fragen der betrieblichen Ordnung und des Verhaltens**“) betroffen sein.
- Oftmals ist umstritten, wo die Grenzen der betrieblichen Mitbestimmung beim Beschäftigtendatenschutz liegen und ob der Betriebsrat bei allgemeinen datenschutzrechtlichen Fragen bzgl. des Umgangs mit Beschäftigtendaten mitzubestimmen hat.

I. Reichweite der erzwingbaren Mitbestimmung

2. Technische Überwachung nach § 87 Abs. 1 Nr. 6 BetrVG (1)

- § 87 Abs. 1 Nr. 6 BetrVG enthält einen weiten Überwachungsbegriff, sodass schon in alltäglichen Situationen des Arbeitslebens eine mitbestimmungsrelevante Überwachung vorliegen kann.
- Eine technische Überwachung liegt bereits dann vor, wenn die **Einrichtung objektiv zur Überwachung geeignet** ist. Es kommt nicht auf die subjektive Absicht des Arbeitgebers an, Mitarbeiter zu überwachen. Entscheidend ist, ob sich objektiv Rückschlüsse auf die Leistung oder das Verhalten der Beschäftigten durch das technische Mittel ziehen lassen können.
- Eine technische Überwachung nach § 87 Abs. 1 Nr. 6 BetrVG liegt dann nicht vor, wenn sich die Kontrolle technisch ausschließen lässt.

I. Reichweite der erzwingbaren Mitbestimmung

2. Technische Überwachung nach § 87 Abs. 1 Nr. 6 BetrVG (2)

- Als Beispiele für technische Überwachungseinrichtungen lassen sich anführen:
 - Videoüberwachung am Arbeitsplatz
 - Einsatz von Microsoft 365
 - Zeiterfassungs- und Zugangskontrollsysteme
 - IT-Antivirus – und Spamfilterprogramme

I. Reichweite der erzwingbaren Mitbestimmung

3. Betriebliche Ordnung und Verhalten nach § 87 Abs. 1 Nr. 1 BetrVG (1)

- Bei nicht-technischen Kontrollen am Arbeitsplatz kann auch das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 1 BetrVG betroffen sein.
- Gleiches gilt für Verhaltensregeln, die den Umgang mit IT-Kommunikationsmitteln am Arbeitsplatz betreffen und damit mittelbar im Zusammenhang mit Beschäftigtendaten stehen.
- So ist die zeitliche Beschränkung der Privatnutzung des betrieblichen Internet- und/oder Email-Zugangs mitbestimmungspflichtig (das „wie“ ist betroffen).
- Dagegen ist das Verbot der Privatnutzung des dienstlichen Internet- und/oder Email-Zugangs mitbestimmungsfrei (das „ob“ ist betroffen).

I. Reichweite der erzwingbaren Mitbestimmung

3. Betriebliche Ordnung und Verhalten nach § 87 Abs. 1 Nr. 1 BetrVG (2)

- Als Beispiele für Fragen der betrieblichen Ordnung oder des Verhaltens der Arbeitnehmer im Betrieb nach § 87 Abs. 1 Nr. 1 BetrVG lassen sich anführen:
 - Tor- und Taschenkontrollen
 - Lösungs- und Kennzeichnungspflichten privater Emails
 - Aufstellung von KI- oder Social-Media Guidelines, die die berufliche Nutzung regeln sollen
 - zeitliche Beschränkung der Privatnutzung betrieblicher Kommunikationsmittel

I. Reichweite der erzwingbaren Mitbestimmung

4. Grenzen der erzwingbaren Mitbestimmung (1)

- Häufig ufern Verhandlungen mit Betriebsräten über Detailfragen des Datenschutzes aus. Der Betriebsrat sieht sich regelmäßig als „Hüter des Datenschutzes“ und möchte oft über viele Einzelheiten des Datenschutzes mitbestimmen.
- Datenschutzrecht allein und die Erfüllung der DSGVO-Pflichten durch den Arbeitgeber ist kein Teil der erzwingbaren Mitbestimmung. **Die erzwingbare Mitbestimmung aus § 87 Abs. 1 Nr. 6 BetrVG beschränkt sich auf Leistungs- und Verhaltensdaten.**
- Nicht die Einhaltung von Datenschutzbestimmungen ist Bestandteil der Mitbestimmung sondern der reine Persönlichkeitsschutz der Mitarbeiter.
- Die erzwingbare Mitbestimmung soll Mitarbeiter vor Überwachung schützen und hat nicht die Einhaltung des Datenschutzrechts zu gewährleisten.

I. Reichweite der erzwingbaren Mitbestimmung

4. Grenzen der erzwingbaren Mitbestimmung (2)

- Die Mitbestimmung bezieht sich daher nicht pauschal auf die Zweckbestimmung der Datenverarbeitung, Erforderlichkeit der Datenverarbeitung oder der Zugriffsberechtigung „Need-to-know-Prinzip“.
- Um das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG zu eröffnen, muss immer ein **spezifischer Aspekt von Mitarbeiterüberwachung** betroffen sein.
- So hat das BAG ein **MBR nach § 87 Abs. 1 Nr. 6 BetrVG beim Anti-Terror-Listen-Screening abgelehnt**, da keine unmittelbare Überwachung von Leistung oder Verhalten vorlag (BAG 19.12.2017 – 1 ABR 31/16).
- Nach dem LAG Hessen war die **umfassende Regelung aller Einzelheiten eines IT-Systems**, die datenschutzrechtskonforme Datenverarbeitung sowie die Übermittlung von Beschäftigtendaten in einen Drittstaat **nicht mitbestimmungspflichtig**, da es an einem unmittelbaren Überwachungsbezug fehlte (LAG Hessen 5.12.2024 – 5 TaBV 4/24).
- Nach dem LAG Hessen bezieht sich § 87 Abs. 1 Nr. 6 BetrVG nicht auf die Einhaltung der DSGVO oder auf die Ausgestaltung von datenschutzrechtlichen Pflichten des Arbeitgebers. Der Betriebsrat ist hier auf seine Überwachungsaufgaben nach § 80 Abs. 1 Nr. 1 BetrVG und Unterrichtsrechte nach § 80 Abs. 2 BetrVG beschränkt.

I. Reichweite der erzwingbaren Mitbestimmung

4. Grenzen der erzwingbaren Mitbestimmung (3)

Praxisbeispiele, bei denen **gegen ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG** argumentiert werden kann und im Umkehrschluss nur Beteiligungsrechte aus § 80 BetrVG bestehen:

- 1) **Datenverarbeitung aufgrund des Verdachts von Straftaten**; ausdrücklich durch § 26 Abs. 1 S. 2 BDSG geregelt; damit ist die Mitbestimmung schon aus § 87 Abs. 1 Es BetrVG ausgeschlossen.
- 2) **Reine Verarbeitung von Arbeitnehmer-Statusdaten** (zB Stammdaten, Funktion, Steuerdaten) ermöglichen keine Kontrolle des Mitarbeiters; damit besteht kein Mitbestimmungsrecht.
- 3) **Reine Zugriffs- und Berechtigungskonzepte**, bei denen tabellarisch dargestellt wird, wer auf welche Daten zugreifen darf, stellen ein Verarbeitungsverzeichnis nach Art. 30 I lit. d) DSGVO dar, dass durch organisatorische Maßnahmen nach Art. 32 DSGVO erfüllt wird. Eine Mitbestimmung scheidet demnach nach § 87 Abs. 1 Es BetrVG aus (anders ist dies allerdings, wenn bei konkreten Kontrollauswertungen ein Verfahrensprozess verarbeitet wird, der auch festlegt, welcher Personenkreis zu welchem Zeitpunkt in die Auswertung involviert wird; MBR hier dann +).

I. Reichweite der erzwingbaren Mitbestimmung

4. Grenzen der erzwingbaren Mitbestimmung (4)

Praxisbeispiele, bei denen **gegen ein Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG** argumentiert werden kann und im Umkehrschluss nur Beteiligungsrechte aus § 80 BetrVG bestehen:

- 4) **Schnittstellentechnik** hat keine überwachende Funktion; fungiert als informationstechnologische Brücke, die selbst keine Daten analysiert oder auswertet; Mitbestimmungsrecht scheidet damit aus.
- 5) **Datentransfers aus oder in Drittländer** sind nicht mitbestimmungspflichtig. Das BetrVG ist schon bei Datenverarbeitungsvorgängen in anderen Ländern nicht anwendbar („Territorialitätsprinzip“). Ein Mitbestimmungsrecht kommt nur bei Datenübermittlungen aus Deutschland heraus in Betracht. Die Datenübermittlung in Drittstaaten ist durch Art. 44 ff. DSGVO geregelt, sodass eine Mitbestimmung schon wegen § 87 Abs. 1 Es BetrVG ausscheidet. Zudem stellt der reine Datentransfer in Drittstaaten keinen Bezug zur unmittelbaren Mitarbeiterüberwachung her.

I. Reichweite der erzwingbaren Mitbestimmung

5. Beweisverwertungsverbote als Teil der Mitbestimmung? (1)

- Aus **alleinigen Verstößen gegen die Mitbestimmungsrechte** des Betriebsrats resultiert **kein prozessuales Beweisverwertungsverbot** (vgl. BAG 29.6.2023 – 2 AZR 296/22; BAG 13.12.2007 – 2 AZR 537/06).
- Für ein prozessuales Beweisverwertungsverbot ist vielmehr notwendig, dass ein erheblicher Eingriff in das Persönlichkeitsrecht des betroffenen Mitarbeiters stattgefunden hat (z.B. unzulässige Kontrolle am Arbeitsplatz, durch die unverhältnismäßig in die Persönlichkeitssphäre eingegriffen wurde).
- Es existiert allerdings **kein absolutes Beweisverwertungsverbot bei Eingriffen in das Persönlichkeitsrecht**. Findet eine „einfache“ Persönlichkeitsrechtsverletzung statt und wurde mit einer Kontrolle ein Straftatverdacht erfolgreich aufgeklärt, kann ein Beweisverwertungsverbot ausscheiden (BAG-Linie hierzu: „**Datenschutz ist kein Tatenschutz**“).
- Ein alleiniger Verstoß gegen Mitbestimmungsrechte kann in jedem Fall kein prozessuales Beweisverwertungsverbot rechtfertigen, da dadurch „nur“ in die Rechte des Betriebsrats und nicht in das Persönlichkeitsrecht des Mitarbeiters eingegriffen wird. **Der Persönlichkeitsschutz kann nicht über die Beteiligungsrechte des Betriebsrats erweitert werden.**

I. Reichweite der erzwingbaren Mitbestimmung

5. Beweisverwertungsverbote als Teil der Mitbestimmung? (2)

- In Betriebsvereinbarungen wird häufig geregelt, dass Datenverarbeitungen zum Zweck einer Leistungs- und Verhaltenskontrolle ausgeschlossen sein sollen oder eine vorherige zwingende Zustimmung des Betriebsrats zu erfolgen hat. Zudem soll bei Verstößen gegen die Betriebsvereinbarung häufig ein Sachvortrags- und Beweisverwertungsverbot greifen.
- In einer BV wurde zB geregelt:
 - (1) *„...dürfen nicht zur Kontrolle von Leistung und Verhalten der Mitarbeiter herangezogen werden. Eine Auswertung kann nur in begründeten Fällen (zB konkreter Straftatverdacht) im Einvernehmen mit dem Betriebsrat erfolgen.*
 - (2) *Besteht kein Einvernehmen, unterbleibt die Auswertung. Der Arbeitgeber ist in diesem Fall die Herbeiführung einer gerichtlichen Entscheidung vorbehalten...Erfolgt eine Auswertung ohne das Vorliegen des Einvernehmens mit dem Betriebsrat, unterliegen alle hierbei gewonnenen Erkenntnisse einem Beweisverwertungsverbot. Sie dürfen insbesondere nicht für arbeitsrechtliche Maßnahmen wie Abmahnungen oder Kündigungen genutzt werden“.*

I. Reichweite der erzwingbaren Mitbestimmung

5. Beweisverwertungsverbote als Teil der Mitbestimmung? (3)

- Die vorher dargestellte Regelung der BV ist unwirksam. **BVen können keine absoluten Verbote von Leistungs- und Verhaltenskontrollen regeln und auch keine Verwertungsverbote statuieren.**
- Es bestehen dafür **keine gesetzlichen Mitbestimmungsrechte** des Betriebsrats bzw. **keine Regelungsbefugnis der Betriebsparteien** (vgl. BAG 29.6.2023 – 2 AZR 296/22; LAG Hessen 12.6.2025 – 5 TaBV 134/24). Es besteht eine Unvereinbarkeit mit Prozessrecht (ZPO/StPO).
- Auf das Recht zur fristlosen Kündigung kann individualvertraglich nicht verzichtet bzw. nicht erheblich erschwert werden; ein solche Regelung ist nach § 134 BGB nichtig. BV-Regelungen, die Verhaltenskontrollen ausschließen oder Verwertungsverbote festlegen, erschweren wegen der Ausschlussfrist nach § 626 Abs. 2 BGB erheblich eine fristlose Kündigung (Argument für die Nichtigkeit der Regelung).
- Zudem können solche Regelungen auch Verstöße gegen die Unternehmenspflicht zur Sicherstellung der Compliance begründen (zB §§ 130, 30 OWiG, 43 GmbHG, 93 AktG). Eine derartige **Pflichtenkollision zwischen BV-Regelungen und gesetzlichen Compliance-Pflichten ist nicht hinnehmbar.**

II. Gestaltungsmöglichkeiten einer BV als Erlaubnisnorm

1. Formelle Voraussetzungen für eine DSGVO-Erlaubnisnorm (1)

- Auf Grundlage von Art. 88 Abs. 1 DSGVO und § 26 Abs. 4 S. 1 BDSG kann eine Betriebsvereinbarung grds. als datenschutzrechtliche Erlaubnisnorm ausgestaltet werden.
- In formeller Hinsicht sind die **Vorgaben aus Art. 88 Abs. 2 DSGVO** zu beachten:
 - (1) Es sind angemessene Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte des Betroffenen zu treffen:
 - (2) Die Grundprinzipien der DSGVO aus Art. 5 DSGVO müssen beachtet und in der BV sollte auf sie hingewiesen werden.
 - (3) Die Betroffenenrechte aus Art. 12 ff. DSGVO müssen abgebildet sein.
 - (4) Die BV sollte ausdrücklich als datenschutzrechtliche Erlaubnisnorm definiert werden.
 - (5) Umsetzung der Transparenzvorgaben aus Art. 88 Abs. 2 DSGVO (zB durch klare und verständliche Regelungen)

II. Gestaltungsmöglichkeiten einer BV als Erlaubnisnorm

1. Formelle Voraussetzungen für eine DSGVO-Erlaubnisnorm (2)

- Die formellen Voraussetzungen des Art. 88 Abs. 2 DSGVO gelten auch für BVen, die vor Anwendbarkeit der DSGVO abgeschlossen wurden und als Erlaubnisnorm wirken sollten (es gibt **keinen Bestandsschutz**).
- Dies kann sich insbesondere nachteilig für „alte“ BVen auswirken, die zum konzernweiten Datenaustausch abgeschlossen wurden (wegen fehlendem Konzernprivileg diente oftmals BV als Rechtfertigungsgrundlage).
- BVen sollten daher an Voraussetzungen des Art. 88 Abs. 2 DSGVO angepasst werden, wenn sie als Erlaubnisnorm wirken sollen. Es kann sich auch der Abschluss einer RahmenBV anbieten, die die formellen Voraussetzungen des Art. 88 Abs. 2 DSGVO den Bestands-BVen „überstülpt“.
- Die Gestaltung einer BV als Erlaubnisnorm stellt keine erzwingbare Mitbestimmung aus § 87 Abs. 1 BetrVG dar und kann daher nicht gegen den Willen der anderen Betriebspartei durchgesetzt werden

II. Gestaltungsmöglichkeiten einer BV als Erlaubnisnorm

2. Unterschreitung der DSGVO durch BV als Erlaubnisnorm? (1)

- Vor Anwendbarkeit der DSGVO war es anerkannt, dass eine Betriebsvereinbarung vom Schutzstandard des „alten“ BDSG abweichen und „eigenes“ Datenschutzrecht setzen konnte (vgl. u.a. BAG 9.7.2013 – 1 ABR 2/13).
- Bisher war man davon ausgegangen, dass eine BV auch vom Schutzstandard der DSGVO nach unten abweichen kann, da eine Erlaubnisnorm spezifische Regelungen im Vergleich zur DSGVO enthalten muss („unionsrechtliches Wiederholungsverbot“).
- Der EuGH hat allerdings entschieden, dass **eine BV nicht „nach unten“ vom DSGVO-Schutzstandard abweichen darf** (EuGH 19.12.2024 –C-65/23). Demnach darf eine Betriebsvereinbarung nicht weiter in die Persönlichkeitsrechte der Mitarbeiter eingreifen, als es die DSGVO zulässt.
- Die EuGH-Entscheidung ist kritisch dahingehend zu hinterfragen, inwiefern nach diesen Maßstäben eine BV als Erlaubnisnorm nach Art. 88 DSGVO wirken und spezifische Regelungen enthalten kann, um nicht gegen das Wiederholungsverbot zu verstoßen.

II. Gestaltungsmöglichkeiten einer BV als Erlaubnisnorm

2. Unterschreitung der DSGVO durch BV als Erlaubnisnorm? (2)

- Trotz der EuGH-Rechtsprechung ist es zu empfehlen, **Betriebsvereinbarungen in datenschutzrechtlich sensiblen Angelegenheiten als Erlaubnisnorm auszugestalten** (sofern der Betriebsrat mitwirkt).
- Gerade beim **umfangreichen konzernweiten Datenaustausch** ist eine BV als Erlaubnisnorm faktisch alternativlos („kleines“ Konzernprivileg nach EG 48 zur DSGVO oder Auftragsverarbeitung helfen nur bedingt weiter).
- Zudem können sich viele Beschäftigtendatenverarbeitungen oder Kontrollmaßnahmen am Arbeitsplatz im rechtlichen Graubereich bewegen (wegen Interessenabwägung im konkreten Einzelfall).
- Eine **BV als Erlaubnisnorm** verschafft – unabhängig von der EuGH-Rechtsprechung – in **Graubereichsfällen argumentativen Spielraum gegenüber Datenschutzaufsichtsbehörden und Arbeitsgerichten**, so dass sich die Datenverarbeitung als noch rechtmäßig erweisen kann.
- Hart verhandelte BV unter Betriebsparteien auf Augenhöhe sorgt aus Sicht der Behörden und Gerichte für mehr Ausgewogenheit, als wenn die Datenverarbeitung einseitig durch den Arbeitgeber angeordnet wurde.

III. Pflichten des Betriebsrats nach § 79a BetrVG

1. Betriebsrat (nur) Teil der verantwortlichen Stelle

- Vor Schaffung des § 79a BetrVG war umstritten, ob der Betriebsrat seit Anwendbarkeit der DSGVO datenschutzrechtlich als verantwortliche Stelle mit allen damit verbundenen Pflichten einzustufen ist.
- § 79a S. 2 BetrVG hat diese Frage dahingehend entschieden, dass der Arbeitgeber alleiniger Verantwortlicher bleibt und der **Betriebsrat nur Teil der verantwortlichen Stelle** ist.
- Dem Arbeitgeber treffen damit die datenschutzrechtlichen Pflichten wie Erfüllung der DSGVO-Betroffenenrechte, Bestellung eines Datenschutzbeauftragten oder Erstellung eines Verarbeitungsverzeichnisses alleine.
- Für den Betriebsrat gelten diese DSGVO-Pflichten mangels Stellung als Verantwortlicher nicht. Der **Betriebsrat hat allerdings bei der Erfüllung seiner Aufgaben die datenschutzrechtlichen Vorgaben zu beachten**. Auch über § 75 Abs. 2 BetrVG wird der Betriebsrat zur Beachtung der Persönlichkeitsrechte der Arbeitnehmer verpflichtet.

III. Pflichten des Betriebsrats nach § 79a BetrVG

2. DSGVO-Vorgaben für den Betriebsrat in der Praxis (1)

In der Praxis gibt es zahlreiche Konstellationen, bei denen sich der Betriebsrat an datenschutzrechtliche Vorgaben zu halten hat. Hierunter fallen zB:

- **Verbot der unzulässigen Vorratsdatenspeicherung**; dem Betriebsrat ist es verwehrt, eine eigene Personaldatei aufzubauen;
- der Betriebsrat hat die ihm anvertrauten Beschäftigtendaten zu löschen, sobald er diese für die Aufgabenerfüllung nicht mehr benötigt (eine **dauerhafte Speicherung ist ausgeschlossen**);
- **Umsetzung von technischen und organisatorischen Maßnahmen** nach Art. 24, 32 DSGVO, um einen DSGVO-konformen Umgang mit den anvertrauten Beschäftigtendaten sicherzustellen (insb. bei besonderen Kategorien personenbezogener Daten wie Schwangerschaften, Gesundheitsdaten, Schwerbehinderung, etc.; vgl. u.a. BAG 9.4.2019 – 1 ABR 51/17);

III. Pflichten des Betriebsrats nach § 79a BetrVG

2. DSGVO-Vorgaben für den Betriebsrat in der Praxis (2)

- Auch die Vielzahl an **gesetzlichen Verschwiegenheitsverpflichtungen** führt dazu, dass der Betriebsrat den Datenschutz bei seiner Aufgabenerfüllung umzusetzen hat.
- Der Betriebsrat bzw. seine Mitglieder dürfen **personenbezogenen Daten nur im Rahmen ihrer BetrVG-Aufgaben verarbeiten**.
- Weiter trifft den Betriebsrat seine **allgemeine Verschwiegenheitsverpflichtung aus § 79 BetrVG**. Betriebs- und Geschäftsgeheimnisse, die der Arbeitgeber als geheimhaltungsbedürftig bezeichnet hat, fallen hierunter.
- Über § 99 Abs. 1 S. 3 BetrVG sind Betriebsratsmitglieder **bzgl. personeller Einzelmaßnahmen verpflichtet**, über die bekannt gewordenen persönlichen Verhältnisse von Mitarbeitern oder Bewerbern **Verschwiegenheit zu wahren**. Hier bedarf es keiner ausdrücklichen Geheimhaltungserklärung des Arbeitgebers.
- **Weitere Geheimhaltungsverpflichtungen** des Betriebsrats folgen aus §§ 102 Abs. 2 S. 5, 82 Abs. 2 S. 3 oder § 83 Abs. 1 S. 2 BetrVG.

III. Pflichten des Betriebsrats nach § 79a BetrVG

3. Folgen für den Betriebsrat bei Datenschutzverstößen (1)

- Sofern der Betriebsrat im Rahmen seiner Aufgabenerfüllung personenbezogene Daten verarbeitet und es dabei zu DSGVO-Verstößen kommt, **haftet der Arbeitgeber als Verantwortlicher**.
- Der Arbeitgeber ist daher Adressat von Bußgeldbescheiden durch die Datenschutzaufsichtsbehörden und gegen ihn richten sich grds. auch Schadenersatzansprüche der Betroffenen nach Art. 82 DSGVO.
- DSGVO-Verstöße, die ausschließlich oder weit überwiegend in der Sphäre des Betriebsrats zu suchen sind, können haftungsmildernd oder sogar zu einem Haftungsentfall des Arbeitgebers führen, da er nur bedingt Einfluss auf die DSGVO-Prozesse des Betriebsrats nehmen kann.
- Die **Stellung des Arbeitgebers als Verantwortlicher bleibt jedoch wegen § 79a BetrVG unberührt**.

III. Pflichten des Betriebsrats nach § 79a BetrVG

3. Folgen für den Betriebsrat bei Datenschutzverstößen (2)

- **Handelt der Betriebsrat** allerdings bei der Datenverarbeitung **außerhalb seiner Zuständigkeit, entfällt eine Verantwortlichkeit des Arbeitgebers** nach § 79a S. 2 BetrVG. Der Arbeitgeber ist in solchen Fällen nicht mehr Adressat von Bußgeldbescheiden der Aufsichtsbehörden.
- Eine **Haftung des Betriebsrats als Organ scheidet wegen Vermögenslosigkeit aus**. Dagegen kann eine Haftung von einzelnen Betriebsratsmitgliedern oder einer Gruppe in Betracht kommen, wenn der DSGVO-Verstoß sich auf diese Personen zurückzuführen lässt („Datenexzesse“ von Betriebsratsmitgliedern).
- Eine **persönliche Haftung von Betriebsratsmitgliedern** kommt allerdings nur bei schwerwiegenden Datenschutzverstößen in Betracht. Zudem darf die persönliche Haftung nicht zu unangemessenen finanziellen Nachteilen führen, da dies mit dem BR-Ehrenamtsprinzip nicht vereinbar wäre. Dies ist bei der Bemessung von Bußgeldern durch die Aufsichtsbehörden und/oder Gerichten zu berücksichtigen.

III. Pflichten des Betriebsrats nach § 79a BetrVG

3. Folgen für den Betriebsrat bei Datenschutzverstößen (3)

- Bei erheblichen DSGVO-Verstößen kommt auch der **Ausschluss eines einzelnen BR-Mitglieds** oder sogar die Auflösung des BR-Gremiums nach § 23 Abs. 1 BetrVG in Betracht. Dies gilt für Datenverarbeitungsvorgänge, die der Betriebsrat im Rahmen seiner BR-Tätigkeit begangen hat.
- Hat ein Betriebsratsmitglied außerhalb seiner BR-Tätigkeit erhebliche Datenschutzverstöße im Rahmen seines Arbeitsverhältnisses begangen, scheidet § 23 Abs. 1 BetrVG aus und es kommt eine **fristlose Kündigung** in Betracht, die der Zustimmung des Betriebsrats nach § 103 BetrVG unterliegt.
- Bei DSGVO-Verstößen kann zugleich eine Verletzung von Amts- und Vertragspflichten (zB schwerer Vertrauensverlust, Verletzung von internen Datenschutzvorgaben, etc.) vorliegen. In solchen Fällen kann neben den Antrag auf Ausschluss aus dem BR-Gremium auch der parallele Ausspruch einer fristlosen Kündigung in Betracht kommen.
- Das LAG Hessen hat die Weiterleitung von sensiblen Personaldaten vom dienstlichen an den privaten E-Mail-Account des Betriebsratsvorsitzenden als grober Pflichtverletzung eingestuft und damit den Ausschluss aus dem BR-Gremium bejaht (LAG Hessen 10.3.2025 – 16 TaBV 109/24).

III. Pflichten des Betriebsrats nach § 79a BetrVG

4. Kontrolle der DSGVO-Pflichten des Betriebsrats (1)

- Der Arbeitgeber kann nicht unmittelbar kontrollieren, inwiefern der Betriebsrat seine DSGVO-Pflichten beachtet. Der Betriebsrat ist bei Erfüllung seiner Aufgaben unabhängig und damit weisungsfrei.
- § 79a S. 3 BetrVG regelt allerdings, dass sich **Arbeitgeber und Betriebsrat bei der Erfüllung der datenschutzrechtlichen Pflichten gegenseitig unterstützen**.
- Aus dieser Unterstützungspflicht folgt, dass der Arbeitgeber verlangen kann, dass der Betriebsrat ihm die Informationen erteilt, aus denen sich die Umsetzung der technisch und organisatorischen Maßnahmen nach Art. 24, 32 DSGVO ergibt. Zudem hat der Betriebsrat die Informationen aus seiner Sphäre zu übermitteln, die der Arbeitgeber für die Erstellung des Verarbeitungsverzeichnisses, der Informationsblätter nach Art. 13 DSGVO oder zur Erfüllung des Auskunftsanspruchs nach Art. 15 DSGVO benötigt.
- Zudem hat der Betriebsrat gegenüber dem Arbeitgeber darzulegen, zur Erfüllung welcher konkreten BetrVG-Pflichten er Beschäftigtendaten benötigt.
- Bei Verletzungen der Unterstützungspflichten nach § 79a S. 3 BetrVG, kann der Arbeitgeber gegen den Betriebsrat nach § 23 Abs. 1 BetrVG vorgehen.

III. Pflichten des Betriebsrats nach § 79a BetrVG

4. Kontrolle der DSGVO-Pflichten des Betriebsrats (2)

- Mit guten Argumenten lässt sich vertreten, dass der **Datenschutzbeauftragte den Betriebsrat bzgl. der Erfüllung der DSGVO-Pflichten kontrollieren** kann. Rechtsprechung zu dieser Frage ist allerdings (noch) nicht ersichtlich.
- Früher wurde vertreten, dass der DSB den Betriebsrat nicht kontrollieren kann, da er als Vertreter des Arbeitgebers einzustufen sei. § 79a S. 4 BetrVG regelt nun allerdings, dass der DSB gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet ist, was Rückschlüsse auf den Meinungsbildungsprozess des BR zulässt.
- § 79a S. 4 BetrVG setzt damit impliziert voraus, dass der DSB den Betriebsrat kontrollieren kann, sonst wäre diese Regelung überflüssig.
- Im Einklang damit steht auch die BAG-Rechtsprechung, wonach die Stellung als BR-Vorsitzender nicht mit der Funktion als DSB vereinbar ist. Danach legt der BR Mittel und Zwecke seiner Datenverarbeitung fest, sodass dies im Widerspruch zum grundsätzlichen Kontrollauftrag des DSB steht (BAG 6.6.2023 – 9 AZR 383/19).

IV. Beteiligungsrechte BR vs. AN-Persönlichkeitsrechte

Wo liegen die rechtlichen Grenzen? (1)

- Oftmals fordern Betriebsräte, dass sie bei konkreten Kontrollmaßnahmen am Arbeitsplatz, Personalgesprächen oder bei der Auswertung von Leistungsdaten automatisch hinzuziehen sind. Wird der Betriebsrat hier ausufernd und ohne ausdrückliches Einverständnis der betroffenen Arbeitnehmer beteiligt, bestehen datenschutzrechtliche Risiken,
- Nach § 75 Abs. 2 BetrVG sind Arbeitgeber und Betriebsrat verpflichtet, die Persönlichkeitsrechte der Mitarbeiter zu schützen. Daneben hat das BVerfG im „Volkszählungsurteil“ aus dem Jahr 1983 das Grundrecht auf informationelle Selbstbestimmung geschaffen, dass auch unter Privaten und damit im Arbeitsverhältnis gilt.
- Zudem können sich Mitarbeiter im Arbeitsverhältnis uneingeschränkt auf ihre Rechte aus der DSGVO und des BDSG berufen.
- Aus diesen Gründen ist ein **angemessener Ausgleich zwischen den Beteiligungsrechten des Betriebsrats und Persönlichkeitsrechten der Mitarbeiter** zu treffen.

IV. Beteiligungsrechte BR vs. AN-Persönlichkeitsrechte

Wo liegen die rechtlichen Grenzen? (2)

- Die umfassende Einbindung des Betriebsrats bei konkreten Kontrollmaßnahmen kann zu erheblichen **datenschutzrechtlichen Risiken und auch zu prozessualen Beweisverwertungsverböten** in Kündigungsschutzprozessen zum Nachteil des Arbeitgebers führen.
- Beim sog. „**Spindurteil**“ des BAG erfolgte eine heimliche Spindkontrolle u.a. deshalb rechtswidrig und unterlag einem Beweisverwertungsverbot, weil ein BR-Mitglied zur Kontrolle hinzugezogen wurde und damit der in die Kontrolle involvierte Personenkreis datenschutzrechtlich zu umfassend war (BAG 20.6.2013 – 2 AZR 546/12).
- Das BAG führte hier u.a. wörtlich aus:

„Die – bestrittene - Behauptung der Beklagten, ihre Vorgehensweise sei mit 2 BR-Mitgliedern abgestimmt gewesen, von denen eines an der Kontrolle teilgenommen habe, rechtfertigt kein anderes Ergebnis. Aus persönlichkeitsrechtlicher und datenschutzrechtlicher Sicht ist der Eingriff deshalb nicht weniger intensiv. Vielmehr ist davon auszugehen, dass die Privatsphäre des Arbeitnehmers umso stärker verletzt wird, je mehr Personen ohne sein Einverständnis an dem Eingriff beteiligt sind.“

IV. Beteiligungsrechte BR vs. AN-Persönlichkeitsrechte

Wo liegen die rechtlichen Grenzen? (3)

- Auch Regelungen, wonach der **Betriebsrat automatisch bei allen Personalgesprächen mit potentiell nachteiligem Charakter teilnimmt** (zB Verdachtsanhörung, Compliance-Interview, etc.), sind **datenschutzrechtswidrig**. Es ist hier vielmehr das ausdrückliche Einverständnis des betroffenen Arbeitnehmers notwendig (BAG 11.12.2018 – 1 ABR 12/17).
- In den Leitsätzen zu der BAG-Entscheidung vom 11.12.2018 wird ausgeführt:
„Eine Regelung in einer Betriebsvereinbarung, nach der ein Arbeitgeber zu einem Personalgespräch, das er mit einem Arbeitnehmer führt, bevor er auf Grund eines diesem vorgeworfenen Fehlverhaltens eine arbeitsrechtliche Maßnahme ergreift, gleichzeitig auch den Betriebsrat zu laden hat, ist nach § 75 Abs. 2 BetrVG unwirksam“ (BAG 11.12.2018, ZD 2019, 320).
- Gleiches gilt für das **BEM-Verfahren nach § 167 Abs. 2 SGB IX**. Auch hier kann der Betriebsrat nur auf ausdrücklichen Wunsch des Mitarbeiters hinzugezogen werden (BAG 19.11.2019 – 1 ABR 36/18). Andernfalls wird der Arbeitnehmer zum fremdbestimmten Objekt degradiert und es findet ein erheblicher Eingriff in sein Persönlichkeitsrecht statt.