PRODATIS®

The eBusiness Solution Company.

DSGVO: Anforderungen an Betriebsvereinbarungen

DSGVO: Anforderungen an Betriebsvereinbarungen

Betriebsvereinbarungen sind ein wichtiges Instrument, um Beschäftigtendaten rechtskonform zu verarbeiten. Wie müssen solche Vereinbarungen ausgestaltet sein, und welche Vorgaben gilt es zu beachten?

Datenschutzbeauftragte (DSB) kommen – etwa im Rahmen ihrer Beratungs- und Überwachungspflichten – an Betriebsvereinbarungen (BV) nicht vorbei.

Denn Betriebsvereinbarungen dienen häufig dazu, Datenverarbeitungen, auch sensibler Art, zu legitimieren und prozesstechnisch auszugestalten.

Betriebsvereinbarungen – auch Gesamt- und Konzern-BV – stellen als Kollektivvereinbarung mögliche Rechtsgrundlagen für die Verarbeitung von Beschäftigtendaten dar.

Das ergibt sich aus Art. 88 Abs. 1 Datenschutz-Grundverordnung (DSGVO) in Verbindung mit § 26 Abs. 4 S. 1 Bundesdatenschutzgesetz (BDSG), zusammen mit Erwägungsgrund 155 DSGVO.

Gleiches gilt im Übrigen für Tarifverträge, Dienstvereinbarungen (beispielweise gemäß § 73 Bundespersonalvertretungsgesetz – BPersVG) und Sprecherausschussrichtlinien (§ 28 Sprecherausschussgesetz – SprAuG).

Beschäftigtendatenschutz – „Öffnungsklausel“

Art. 88 Abs. 1 DSGVO gestattet, dass solche Kollektivvereinbarungen „spezifischere Vorschriften“ aufstellen können, um die Rechte und Freiheiten von Beschäftigten zu schützen. Das Schutzniveau zu reduzieren, ist dadurch ausgeschlossen.

Aus dem Wortlaut ergibt sich auch, dass Kollektivvereinbarungen die allgemeinen Vorschriften der DSGVO (z.B. die Grundsätze aus Art. 5 DSGVO) „nur“ ergänzen, nicht aber verdrängen können.

PRAXIS-TIPP: Manche Betriebsvereinbarungen haben vordefinierte Laufzeiten (sogenannte befristete BV). Diese Laufzeiten sollten der DSB und der Betriebsrat überwachen.

Denn läuft eine BV aus, kann die Rechtsgrundlage für diese Verarbeitung von Beschäftigtendaten entfallen, und die

Rechtmäßigkeit ist vor diesem Hintergrund neu zu prüfen.

Vergleichbares gilt, wenn eine Seite eine Betriebsvereinbarung kündigt oder wenn eine BV abgeschlossen wird, die einen einzelnen, zeitlich begrenzten Sachverhalt regelt.

Typische Verarbeitungssituationen als BV-Gegenstand

Typische Verarbeitungssituationen- / zwecke, die BVs regeln können, finden sich ebenfalls in der Grundverordnung, wenngleich nur sehr rudimentär und nicht abschließend (Art. 88 Abs. 1 DSGVO in Verbindung mit Erwägungsgrund 155).

Die DSGVO nennt die Einstellung, die Erfüllung des Arbeitsvertrags sowie die Gesundheit und Sicherheit am Arbeitsplatz.

Die möglichen Datenverarbeitungen im Unternehmen, die Arbeitgeber und Betriebsrat (BR) über eine BV regeln könnten, sind zahlreich, sodass sie sich nicht abschließend aufzählen lassen.

Klassiker sind beispielsweise die Überwachung von E-Mail und Internet inklusive Privatnutzung, Home bzw. Mobile Office, Profiling, automatisierte Einzelentscheidungen, etwa bei der Bewerberauswahl, Videoüberwachung, GPS-Ortung, Zugangssysteme am Arbeitsplatz, Bring your own Device (BYOD) oder die elektronische Personalakte.

Dazu gehören aber auch auf den ersten Blick unscheinbare Datenverarbeitungen wie die durch smarte Arbeitsgeräte (Kettensägen u.Ä.), die durch zahlreiche Sensoren regelmäßig personenbezogene (Leistungs-)Daten von Beschäftigten verarbeiten.

Hier stellt sich in der Praxis häufig die Frage, ob und wie eine BV derartige Datenverarbeitungen regeln soll bzw. muss.

PRAXIS-TIPP: Um Betriebsvereinbarungen zu erstellen und zu formulieren, ist häufig ein Blick in das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO hilfreich.

Denn hieraus ergeben sie bereits wesentliche Informationen für die zu regelnden Inhalte, etwa alle Zwecke einer konkreten Verarbeitung(-stätigkeit) – vorausgesetzt, die (neue) Datenverarbeitung ist schon entsprechend dokumentiert.

Welche Datenschutzinhalte sind in BV zu regeln?

Welche Anforderungen eine Betriebsvereinbarung in datenschutzrechtlicher Hinsicht erfüllen muss, ergibt sich – wenn auch nur abstrakt – aus Art. 88 Abs. 2 DSGVO.

Danach muss eine BV geeignete und besondere Schutzmaßnahmen für die Betroffenen enthalten.

Das gilt insbesondere im Hinblick auf die Transparenz der Verarbeitung, für Übermittlungen innerhalb einer Unternehmensgruppe oder im Hinblick auf Überwachungssysteme am Arbeitsplatz (z.B. Kamera, Zeiterfassung, Ortungssysteme).

Das bedeutet, dass sich aus der BV, die als Rechtsgrundlage dienen kann, die Schutzmaßnahmen und ihre Geeignetheit selbst ergeben bzw. dass genau das dort geregelt sein muss.

Hier reicht ein bloß allgemeiner Verweis auf die DSGVO oder die Wiederholung des Wortlauts einzelner Vorschriften nicht aus.

Es reicht auch nicht, die Grundsätze „zu beachten". Denn hierbei würde es sich nicht um „besondere Maßnahmen" oder um „besondere Regelungen" handeln.

Die BV muss die Grundsätze in ausdrückliche Regelungen übersetzen, da sie ansonsten für die beteiligten Parteien überhaupt keinen Mehrwert haben.

Allerdings legt Art. 88 Abs. 2 DSGVO nur „Mindestanforderungen" fest; die Maßnahmen in einer BV können also darüber hinausgehen und den Beschäftigtendatenschutz strenger regeln.

Dass die Datenschutzgrundsätze, soweit sie Mindeststan-

dards darstellen und nicht gleichartig für alle BV im Unternehmen gelten, zwingend zu berücksichtigen sind, ergibt sich auch aus § 26 Abs. 5 BDSG.

Er spricht die Maßnahmen, die sicherstellen sollen, dass eine BV die Grundsätze von Art. 5 DSGVO einhält, ausdrücklich an.

Grundsätze	Das heißt für die Betriebsvereinbarung
Transparenz und faire Verarbeitung	Die BV muss zwingend Art, Inhalt und Umfang der Datenverarbeitung, einschließlich der zugrundeliegenden Technik, so konkret wie möglich beschreiben, etwa innerhalb der Beschreibung des.Gegenstands der BV um die zu regelnden Inhalte vollständig erfassen und bewerten zu können. Eine transparente Beschreibung verhindert auch, dass es sich - insbesondere bei Überwachung am Arbeitsplatz - um.verdeckte Maßnahmen handelt, die rechtlich nur schwer bis gar nicht zu rechtfertigen sind.
Zweckbindung als Dreh- und Angelpunkt für spezifische Maßnahmen	Die BV sollte den Zweck bzw. die Zwecke der zu regelnden Datenverarbeitung so konkret wie möglich beschreiben. Bei der Einführung einer elektronischen Personalakte wäre z.B.der Zweck ‚Personalverwaltung nicht konkret genug, da sich hieraus keine spezifischen Maßnahmen herleiten lassen. Um die Zwecke zu ermitteln, hilft ein Blick in das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVD.
Datenminimierung	Hier gehört die gesamte Verarbeitung, die Gegenstand der BV ist, auf den Prüfstand, ob sie wirklich nur die Daten erfasst und verarbeitet, die im Hinblick auf die jeweils festgelegten Zwecke erforderlich sind. Diese Daten müssen auch durch spezifische Maßnahmen geschützt werden. Bei smarten Arbeitsgeräten ist es z.B. regelmäßig nicht erforderlich, die Klarnamen der Mitarbeiter im System zu hinterlegen, das womöglich noch ein externer Dienstleister hostet Es reicht die Personalkennnummer. idealerweise lassen sich Buchstaben technisch bedingt überhaupt nicht eingeben.
Datenrichtigkeit	Hier ist festzulegen, wie (proaktiv und/oder repressiv) gewährleistet werden soll, dass die Daten richtig sind, und wer wann die Daten prüft und berichtigt. Beispiel:‚Eine erforderliche Datenberichtigung (mithin Aktualisierung, sachliche I\nderung und Vervollständigung) im Zusammenhang mit der Nutzung des Systems x wird durch die‚Person/Abteilung/Stelle‘ unter Berücksichtigung der weiteren Datenbanken y vorgenommen, dokumentiert und eine Bestätigung hierrüber an den Beschäftigten übersandt.Ist der Prozess bei allen Datenverarbeitungen, die die BVs regeln, gleich, bietet es sich an, die Berichtigung in einer Rahmen-BV zu regeln.
Speicherdauer und Speicherbegrenzung	Eine BV muss Löschfristen klar definieren. Falls das nicht möglich ist, muss sie zumindest die Kriterien der Löschung (z.B. Löschung der Daten xy nach Beendigung der Horne-Office-Tätigkeit) nennen. Da die erforderliche Speicherdauer je nach Zweck individuell ist, ist dieser Punkt zwingend in jeder BV separat zu regeln.
Integ rität und Vertraulichkeit	Die zu beschreibenden Schutzmaßnahmen variieren häufig, je nach Zweck der Datenverarbeitung.Beispielsweise sind die zugriffsberechtigten Personen und die Voraussetzungen des Zugriffs sowie die Speicherorte (analog/digital) zu definieren. Hierbei bietet es sich an, auf das Konzept der technisch-organisatorischen Maßnahmen des Verantwortlichen zurückzugreifen. Ist ein Auftragsverarbeiter eingebunden, so sind - zumindest für den jeweiligen Verarbeitungsabschnitt- auch dessen Schutzmaßnahmen aufzuführen.

Am Risiko orientieren

Die Schutzvorkehrungen und ihre Regelungstiefe in BV müssen sich am Risiko für die Rechte und Freiheiten der Beschäftigten orientieren, das durch die betreffende Datenverarbeitung besteht.

So dürften beispielsweise die Schutzvorkehrungen und die Regelungstiefe bei der Einführung von elektronischen Kantinenkarten (ohne Speicherung von Zusatzinformationen wie Lebensmittelunverträglichkeiten) geringer ausfallen, als wenn es darum geht, ein unternehmensweites biometrisches Zutritts- oder Zeiterfassungssystem zu implementieren.

Im letzteren Fall würden auch besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO verarbeitet.

Rahmenbetriebsvereinbarungen

Geht es im Unternehmen darum, BV anzupassen, hört man – als DSB oder externer Berater – häufig den Satz: „Wir haben unsere vorhandenen BV durch eine Rahmen-BV an die DSGVO angepasst".

In dieser Absolutheit ist die Aussage rechtlich allerdings nur in Ausnahmefällen korrekt.

Zentraler Merksatz: Alle allgemeinen Regelungen, die für nahezu alle Betriebsvereinbarungen gleich sind, lassen sich in einer Rahmen-BV regeln. Mehr aber auch nicht.

So lassen sich die Informations- oder Auskunftspflichten grundsätzlich abstrakt und in einer für alle BV gültigen Weise regeln.

Das gilt jedoch nicht für die Zwecke, die Speicherdauer oder die spezifischen Schutzmaßnahmen, die je nach Gegenstand der BV höchst unterschiedlich ausfallen können.

Regelmäßig können Rahmenbetriebsvereinbarungen – unter Beachtung von Ausnahmen im Einzelfall – erfahrungsgemäß folgende Punkte regeln:

- Unterrichtungs- und Informationspflichten (Art. 12, 13, und 14 DSGVO), aber für jede Datenverarbeitung hinreichend auszufüllen / zu beschreiben
- Auskunftspflichten (Art. 15 DSGVO)
- Löschung der Daten unter Bezugnahme auf ein bestehendes Löschkonzept (Art. 17 DSGVO) – sofern es alle einbezogenen Daten auch tatsächlich erfasst
- Sicherstellung und Wahrnehmungsmodalitäten der einzelnen Betroffenenrechte, wofür sich auch der Verordnungstext ausschnittsweise verwenden oder umschreiben lässt. Die Betroffenenrechte in jeder einzelnen BV aufzuführen bzw. zu beschreiben, würde den Text überfrachten, sodass er nur noch wenig transparent und verständlich wäre.

Welche Rolle spielt der Betriebsrat in Sachen Datenschutz?

Das Betriebsverfassungsgesetz (BetrVG) enthält keine generelle Mitbestimmungsbefugnis des Betriebsrats für datenschutzrechtlich relevante Sachverhalte (§ 75 und 80 BetrVG).

Es ist vielmehr „lediglich" Aufgabe des BR, die Einhaltung von Datenschutzvorschriften zu überwachen und die Persönlichkeitsrechte der Beschäftigten zu schützen.

Aufgrund allgegenwärtiger Datenverarbeitung im Beschäftigungskontext steht dem BR häufig ein Mitbestimmungsrecht im Hinblick auf technische Einrichtungen zu, mit denen der Arbeitgeber Beschäftigte auch überwachen kann.

Ebenso gewährt § 87 Abs. 1 Nr. 1 BetrVG eine Befugnis zur Mitbestimmung bei allgemeinen Verhaltensregeln zu Datenschutzfragen im Unternehmen.

In diesem Kontext und durch entsprechende BV kann der BR die Einhaltung des Datenschutzrechts fördern.

Die Frage, ob der Betriebsrat als eigener Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO zu qualifizieren ist, thematisiert ausführlich der Beitrag von Dr. Selk in Heft 11/2018, Seite 12–13.

Ausblick
Der zweite Teil des Beitrags beschäftigt sich in der nächsten Ausgabe u.a. mit Konzernbetriebsvereinbarungen, mit dem Umgang mit alten Betriebsvereinbarungen und ihren Anpassungen, häufigen Fehlern in BV sowie mit dem Zusammenspiel zwischen DSB und Betriebsrat.

Wann sind alte BV anzupassen?
Nach überwiegender Auffassung müssen vorhandene BV angepasst werden, wenn die alten Vereinbarungen keine spezifischen Maßnahmen dazu vorsehen, wie sich die einzelnen Datenschutzgrundsätze umsetzen und gewährleisten lassen.

Legt die BV z.B. nicht fest, welche konkreten Maßnahmen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c Datenschutz-Grundverordnung (DSGVO) umsetzen, ist eine Anpassung nötig.

Es gibt allerdings auch die Meinung, es reiche, wenn eine alte BV den Art. 88 Abs. 2 DSGVO und die Grundsätze aus Art. 5 DSGVO nicht verletzt. Schlussendlich muss hier der Europäische Gerichtshof (EuGH) entscheiden.

WICHTIG: Für neue und alte Betriebsvereinbarungen gilt: Sofern sie keine geeigneten und besonderen Maßnahmen zum Schutz der Grund- und Persönlichkeitsrechte der Beschäftigten vorsehen, gehören sie aufgrund des Anwendungsvorrangs der DSGVO in den Papierkorb.

Sie sind keine taugliche Rechtsgrundlage für die Datenverarbeitung.

Das gilt zumindest dann, wenn die BV als spezifischere Rechtsvorschriften im Sinne von Art. 88 Abs. 1 DSGVO fungieren.

Häufige Fehler in alten Betriebsvereinbarungen
Der Anpassungsbedarf für Altbetriebsvereinbarungen ist nach den Erfahrungen des Autors verhältnismäßig groß. Besonders häufig sind folgende Fehler:

- Die Datenverarbeitung ist für die Beschäftigten nicht transparent genug.
- Die zu regelnde Datenverarbeitung ist nur unzureichend und nur ansatzweise beschrieben.
- Die dahinterstehende Technik ist häufig nicht oder nur sehr allgemein beschrieben.
- Die BV enthält keine oder nur eine unzureichende Beschreibung der ergriffenen/zu ergreifenden Schutzmaßnahmen, einschließlich fehlender Hinweise auf die Rechte der Beschäftigten.
- Es finden sich nur allgemeine Klauseln/Verweise zum Datenschutz, statt dass eine konkrete inhaltliche Auseinandersetzung stattfindet.

Wie lassen sich alte BV anpassen?
Hierfür gibt es zwei Wege:

- Einzelprüfung/-anpassung (empfehlenswert, wenngleich mit höherem Aufwand verbunden)
- Rahmenbetriebsvereinbarung und zusätzlich ein spezifischer Steckbrief zum Gegenstand der Datenverarbeitung, der die einzelnen Datenschutzgrundsätze beachtet. Der Steckbrief hat eine konkretisierende Aufgabe. Er muss jede BV bzw. die dahinterstehende Datenverarbeitung individuell aufgreifen und die entsprechenden datenschutzrechtlichen Maßnahmen regeln.

Zusammenspiel von DSB und BR
Der betriebliche DSB spielt auch eine wichtige Rolle bei Betriebsvereinbarungen mit datenschutzrechtlichem Bezug.

Er muss – etwa im Rahmen seiner Beratungspflicht – darauf hinwirken, dass BV, die als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten dienen, den datenschutzrechtlichen Anforderungen genügen sowie die Rechte und Freiheiten der Beschäftigten beachten.
Unabhängig davon, ob – wie in einigen Unternehmen oder öffentlichen Stellen zu beobachten – der DSB den Betriebsrat (BR) in datenschutzrechtlichen Angelegenheiten berät, spielen beide beim Schutz der Persönlichkeitsrechte von Beschäftigten eine wesentliche Rolle.

So sind beide z.B. im Rahmen von Datenschutz-Folgenabschätzungen einzubeziehen; der BR zumindest, sofern es sich um risikoreiche Datenverarbeitungen von Beschäftigtendaten handelt (zur Konsultationspflicht des Verantwortlichen im Rahmen von Datenschutz-Folgenabschätzungen siehe Marschall, Heft 07/2019, S. 17 ff.).

In der Praxis sind häufig gerade solche Datenverarbeitungen Gegenstand von Betriebsvereinbarungen, die einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO unterliegen.

BV als Fundgrube für Datenschutzkontrollen
Insofern sollte sich der Datenschutzbeauftragte mit der wichtigen Frage nach der Rechtskonformität von BV befassen und die Umsetzung überwachen sowie kontrollieren.

Betriebsvereinbarungen bieten ihm zudem zahlreiche Anhaltspunkte für seine Kontroll- und Überwachungspflichten. Sind alle in den BV geregelten Maßnahmen auch tatsächlich umgesetzt?

Ein Praxisfall: Eine Betriebsvereinbarung zum Thema „BEM", also zum betrieblichen Eingliederungsmanagement, legte fest, dass ein Schredder P-5 (DIN 66399) anzuschaffen und zu benutzen ist.

Tatsächlich fühlte sich jedoch niemand im Unternehmen dafür verantwortlich, dieses Gerät auch tatsächlich anzuschaffen. Die Folge: Einige der zu vernichtenden BEM-Dokumente landeten im (normalen) Papierkorb.

Konzernbetriebsvereinbarungen
Die DSGVO beinhaltet – wie das alte Bundesdatenschutzgesetz – kein (generelles) Konzernprivileg. Zugleich nehmen manche mit Hinweis auf Erwägungsgrund 48 DSGVO ein „kleines" Konzernprivileg an.
Denn nach diesem Erwägungsgrund „kann" es sich z.B. bei der Übermittlung von Beschäftigtendaten innerhalb eines Konzerns um ein berechtigtes Interesse des Verantwortlichen handeln.

Das entbindet aber nicht davon, dass für die konzerninterne Übermittlung von Beschäftigtendaten eine Rechtsgrundlage gemäß Art. 6 DSGVO (regelmäßig Buchst. f.) vorliegen muss und Verantwortliche eine Interessenabwägung im Einzelfall durchführen müssen.

Konzernprivileg durch die Hintertür?
Können nun Konzern-BV als Rechtsgrundlage die Datenübermittlung im Konzern generell legitimieren?

Auch Konzern-BV, die den Austausch von Beschäftigtendaten im Konzern regeln, müssen als „spezifischere" nationale Vorschriften im Sinne von Art. 88 Abs. 1 DSGVO zwingend den Voraussetzungen aus Art. 88 Abs. 2 DSGVO sowie den allgemeinen Regelungen der DSGVO entsprechen.

Datenübermittlung nur konkret und für bestimmte Sachverhalte!
Da es nicht möglich ist, dass eine BV das Schutzniveau reduziert, lässt sich ein generelles Konzernprivileg auch nicht durch nationales Recht und damit durch BV einführen oder regeln.

Insofern ist in der Praxis darauf zu achten, dass eine Übermittlung von Beschäftigtendaten in Konzernen stets konkret und auf bestimmte Sachverhalte reduziert ist (z.B. für den Bereich der Personalverwaltung durch die Muttergesellschaft).

Art. 88 Abs. 2 DSGVO verlangt Schutzmaßnahmen bei der Datenübermittlung in Konzernen. Solche Maßnahmen sind in bisherigen Betriebsvereinbarungen nur vereinzelt zu finden. Sie müssen daher angepasst bzw. ergänzt werden.

Fazit: höhere Anforderungen als zuvor
Die Anforderungen, die das Datenschutzrecht an kollektive Regelungen zum Beschäftigtendatenschutz stellt, sind mit Inkrafttreten der DSGVO gestiegen.

Das „Wie" ist in der BV viel entscheidender als das „Ob". Es kommt darauf an, wie (!) eine BV die Persönlichkeitsrechte der Beschäftigten schützt.

Es steht Betriebsrat, Verantwortlichem und Datenschutzbeauftragtem Arbeit ins Haus, sofern alte Betriebsvereinbarungen nicht bereits den Fokus auf datenschutzrechtliche Regelungen gelegt haben.

War der Datenschutz schon vorher zentral, kann auch eine gut austarierte Rahmenvereinbarung ausreichen, um die Anforderungen der Datenschutz-Grundverordnung zu erfüllen.

Neue Betriebsvereinbarungen sollten möglichst gleich mit datenschutzrechtlicher Feder geschrieben werden. Hierzu kann der DSB mit seiner Beratung einen wesentlichen Beitrag leisten.

Quelle:
www.datenschutz-praxis.de