I.M.U.
Institut für Mitbestimmung und Unternehmensführung

Das I.M.U. ist ein Institut der Hans-Böckler-Stiftung

HINTERGRUNDWISSEN

Mai 2019 · Hans-Böckler-Stiftung · Praxiswissen Betriebsvereinbarungen

BESCHÄFTIGTENDATEN-SCHUTZ (DSGVO / BDSG)

Peter Wedde

Darum geht es:
Diese Veröffentlichung soll Betriebs- und Personalräte bei der Anpassung bestehender und neuer Betriebs- und Dienstvereinbarungen an die neuen datenschutzrechtlichen Gegebenheiten unterstützen. Im Mittelpunkt steht das in Kapitel 2 enthaltene Prüfraster, das sowohl stichpunktartige Hinweise für die datenschutzrechtliche Bewertung bestehender und neu abzuschließender Betriebs- und Dienstvereinbarungen als auch Vorschläge für deren inhaltliche Gestaltung enthält. Das Prüfraster ist kein geschlossenes Muster zur unmittelbaren Anwendung, sondern ein Gesamtkatalog mit Hinweisen und Regelungsvorschlägen, die sich auf die wichtigsten Themenfelder beschränken. Auf dieser Basis können Betriebsräte eigene Überlegungen anstellen, Regelungsmodelle entwickeln und individuelle betriebliche Belange berücksichtigen.

Kontakt
Ansprechpartner: Nils Werner
betriebsvereinbarung@boeckler.de
boeckler.de/betriebsvereinbarungen

BETRIEBS-VEREINBARUNGEN

Inhalt

Zusammenfassung

Diese Veröffentlichung soll Betriebs- und Personalräten dabei helfen, bestehende und neue Betriebs- und Dienstvereinbarungen, die die Verarbeitung von Beschäftigtendaten direkt oder indirekt zum Thema haben, an die neuen datenschutzrechtlichen Gegebenheiten anzupassen, die aus der seit dem 25. Mai 2018 wirksamen EU-Datenschutz-Grundverordnung (DSGVO) und aus dem ebenfalls zu diesem Datum in Kraft getretenen neuen Bundesdatenschutzgesetz (BDSG) folgen.
Den Ausführungen zur Prüfung und Gestaltung von Betriebs- und Dienstvereinbarungen werden in Kapitel 1 allgemeine Hinweise zum datenschutzrechtlichen Rahmen vorangestellt. Diese sollen das Verständnis der aufgelisteten Regelungsthemen und ihre datenschutzrechtliche Zuordnung erleichtern.
Im Mittelpunkt der Darstellung steht das in Kapitel 2 enthaltene Prüfraster, das sowohl stichpunktartige Hinweise für die datenschutzrechtliche Bewertung bestehender und neu abzuschließender Betriebs- und Dienstvereinbarungen[i] als auch Vorschläge für deren inhaltliche Gestaltung enthält. Diese Hinweise beziehen sich vorrangig auf Betriebsvereinbarungen zu einzelnen IT-Systemen und auf die hier stattfindende Verarbeitung personenbezogener Daten. Ergänzend enthält Kapitel 3 Hinweise zur Ausgestaltung von einschlägigen „IT-Rahmenvereinbarungen“ bzw. von „Rahmenvereinbarungen zum Beschäftigtendatenschutz“ ergänzt.
Das Prüfraster in Kapitel 2 ist kein geschlossenes Muster zur unmittelbaren Anwendung, sondern ein Gesamtkatalog mit Hinweisen und Regelungsvorschlägen, die sich auf die wichtigsten Themenfelder beschränken. Auf dieser Basis können Betriebsräte eigene Überlegungen anstellen, Regelungsmodelle entwickeln und individuelle betriebliche Belange berücksichtigen.

1 Grundlagen: Der neue datenschutzrechtliche Rahmen für die Ausgestaltung von einschlägigen Betriebsvereinbarungen

Der gesetzliche Rahmen für den Beschäftigtendatenschutz wurde mit den seit dem 25. Mai 2018 geltenden Regelungen der Europäischen Datenschutzgrundverordnung (DSGVO) und des neuen Bundesdatenschutzgesetzes (BDSG) grundlegend erneuert. Diese Erneuerung hat Auswirkungen auf die kollektivrechtliche Gestaltung von betrieblichen Regelungen zum Beschäftigtendatenschutz. Der neue datenschutzrechtliche Rahmen muss sowohl bei der Ausgestaltung von Betriebsvereinbarungen zu einzelnen IT-Systemen als auch bei der Ausgestaltung von Rahmenvereinbarungen zum IT-Einsatz oder zum Beschäftigtendatenschutz beachtet werden.
Arbeitgeber und Betriebsräte sind aus datenschutzrechtlicher Sicht eine Einheit und damit als ein Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO anzusehen. Einer Qualifikation von Betriebsräten als eigenständige Verantwort-

liche steht bereits die Tatsache entgegen, dass sie im Regelfall die vom Arbeitgeber vorgegebenen technischen Mittel für ihre Verarbeitungen nutzen müssen und dass sie zum Umgang mit personenbezogenen Daten nur im Rahmen des BetrVG befugt sind.
Bisher gibt es kein „Mitbestimmungsrecht zum Datenschutz“. Dies verhindert die eigenständige Durchsetzung von Betriebsvereinbarungen zum Datenschutz. Dieses gesetzliche Defizit führt jedoch nicht dazu, dass Betriebsräten die Regelung von Datenschutzthemen damit verschlossen ist. Eine indirekte Regelungsmöglichkeit besteht auf Basis des Mitbestimmungsrechts nach § 87 Abs. 1 Ziff. 6 Betriebsverfassungsgesetz (BetrVG) dann, wenn Arbeitgeber technische Einrichtungen einführen oder ändern wollen, die zur Verhaltens- oder Leistungskontrolle bestimmt sind. Praktisch handelt es sich hierbei um alle IT-Systeme (Hard- oder Software), die im Betrieb eingesetzt werden. Auf der Grundlage ihres Mitbestimmungsrechts können Betriebsräte von Arbeitgebern Festlegungen dazu verlangen, wie datenschutzrechtliche Grundsätze und Regeln bezogen auf bestimmte IT-Systeme umgesetzt werden. Hierzu werden in Abschnitt 1.3 wichtige Einzelthemen vorgestellt.

1.1 Allgemeine Regelungen der DSGVO

Bezogen auf Regelungen zum Beschäftigtendatenschutz müssen bei der Ausgestaltung von Betriebsvereinbarungen die allgemeinen Vorgaben der DSGVO beachtet werden. Hierbei sind Einzelvorschriften der DSGVO herausragend relevant wie etwa

- die in Art. 5 Abs. 1 DSGVO enthalten allgemeinen Grundsätze, die prägend für die Ausgestaltung aller datenschutzrechtlichen Maßnahmen sind;
- die Einhaltung der in Art. 5 Abs. 2 DSGVO bezogen auf diese Grundsätze enthaltene Nachweispflichten des Arbeitgebers als datenschutzrechtlich Verantwortlichen;
- das Vorliegen eines der in Art. 6 Abs. 1 DSGVO abschließend aufgezählten Erlaubnistatbestände;
- das Verbot der Verarbeitung sensibler Informationen aus dem Bereich der besonderen Kategorien personenbezogener Daten in Art. 9 Abs. 1 DSGVO, das allerdings in den in Art. 9 Abs. 2 DSGVO sowie in § 26 Abs. 2 BDSG genannten Fällen durchbrochen wird;
- die Vorgaben in den Art. 12 bis 22 DSGVO zur Wahrung der Rechte der betroffenen Personen;
- die Einhaltungen der gesetzlichen Verpflichtungen zum Datenschutz durch Technikgestaltung in den Art. 24 ff. DSGVO;
- die Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und die Umsetzung der hieraus resultierenden Schutzmaßnahmen, wenn eine Form der Verarbeitung, aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

1.2 Spezifische Vorschriften zum Beschäftigtendatenschutz in der DSGVO und im BDSG

DSGVO und BDSG enthalten spezielle Vorschriften zum Beschäftigtendatenschutz.

- Für die Datenverarbeitung im Beschäftigungskontext eröffnet Art. 88 Abs. 1 DSGVO den Mitgliedsstaaten die Möglichkeit, spezifische Vorschriften zum Beschäftigtendatenschutz durch gesetzliche Regelungen oder durch Kollektivvereinbarungen zu schaffen. Durch Abs. 2 dieses Artikels wird festgelegt, dass diese Vorschriften umfassende angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen enthalten müssen.
- Der durch Art. 88 Abs. 1 DSGVO zur Regelung des Beschäftigtendatenschutzes durch Rechtsvorschriften geschaffene Spielraum ist in Deutschland insbesondere mit § 26 BDSG umgesetzt worden. Die durchgängig novellierten Landesdatenschutzgesetze der Bundesländer enthalten weitgehend textidentische Vorschriften zum Beschäftigtendatenschutz.
- Durch § 26 Abs. 1 Satz 1 BDSG wird die Zulässigkeit der Verarbeitung von Beschäftigtendaten durch Arbeitgeber auf die Fälle der Erforderlichkeit für die Anbahnung, die Durchführung oder die Beendigung der Beschäftigungsverhältnisse begrenzt.
- Basiert eine Verarbeitung auf einer freiwilligen Einwilligung von Beschäftigten im Sinne von Art. 7 DSGVO, muss diese nach § 26 Abs. 2 BDSG immer in Schriftform vorliegen.
- Die allgemeine Erlaubnisnorm in Art. 6 Abs. 1 Buchstabe f) DSGVO lässt eine Verarbeitung von personenbezogenen Daten zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten zu. Hierbei handelt es sich regelmäßig um berechtigte Interessen, die außerhalb der durch § 26 Abs. 1 Satz 1 BDSG begründen Erforderlichkeit angesiedelt sind (etwa die Information eines potentiellen Käufers über die Alters- und Qualifikationsstruktur bestimmter Beschäftigtengruppen). Art. 6 Abs. 1 Buchstabe f) DSGVO ist allerdings kein „Auffangtatbestand“ für die Verarbeitung von Beschäftigtendaten, für die keine Erforderlichkeit i.S.v. § 26 Abs. 1 Satz 1 BDSG besteht und für die es keine andere Rechtsgrundlage gibt. Die Anwendbarkeit dieser Vorschrift setzt allerdings voraus, dass es keine entgegenstehenden überwiegenden Interessen, Grundrechte und Grundfreiheiten der betroffenen Beschäftigten gibt, die den Schutz personenbezogener Daten erfordern. Dies ist im Rahmen einer Verhältnismäßigkeitsprüfung festzustellen. Außerhalb der Erforderlichkeit des § 26 Abs. 1 BDSG ist in diesem Zusammenhang immer von einem Überwiegen der Interessen von Beschäftigten auszugehen. Anwendbar kann Art. 6 Abs. 1 Buchstabe f) DSGVO deshalb nur auf Verarbeitungen sein, die außerhalb des Beschäftigungsverhältnisses stattfinden (etwa die Abwicklung eines Firmenwagenkaufs).

1.3 Praxisbeispiele

In der Praxis können Formulierungen in bestehenden Betriebsvereinbarungen zu datenschutzrechtlichen Problemen führen, die gegen die in Art. 5 Abs. 1 DSGVO enthaltenen Grundsätze verstoßen. Dies gilt beispielsweise für eine Regelung in einer Betriebsvereinbarung zur E-Mail-Nutzung, in der es heißt:

„*Die anfallenden Kommunikationsdaten darf der Arbeitgeber zu Compliance-Zwecken auswerten. Besteht der Verdacht auf Compliance-Verstöße, kann sich die Auswertung auch auf die Inhalte dienstlicher E-Mails erstrecken.*“

Diese sehr allgemein gehaltene Erlaubnisregelung steht im Widerspruch zum Grundsatz der Zweckbindung in Art. 5 Abs. 1 Buchstabe b) DSGVO, der eine Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke zulässt. Der Begriff „Compliance-Zwecke“ erfüllt diesen Grundsatz weder bezogen auf die Eindeutigkeit noch auf die Festlegung bestimmter Kontrollzwecke. Dies wäre ggf. dann anders, wenn nachvollziehbar und abschließend definiert wird, was diese Zwecke sind.
Ähnlich ist eine Regelung zu Kontrollmöglichkeiten in einem Call-Center zu bewerten, in dem es heißt:

„*Der Arbeitgeber ist jederzeit befugt, Telefongespräche zu Zwecken der Qualitätssicherung mitzuhören und die dazugehörigen Aktionen auf dem Bildschirm auszuwerten.*“

Auch dieser Regelung fehlt es an der notwendigen Zweckfestlegung. Sie steht zudem im Widerspruch zum in Art. 5 Abs. 1 Buchstabe a) DSGVO enthaltenen Transparenzgrundsatz, der eine Verarbeitung in einer für die betroffene Person nachvollziehbaren Form einfordert. Dieser Grundsatz ist schon deshalb nicht erfüllt, weil Beschäftigte aufgrund der „jederzeitigen Möglichkeit“ nicht wissen können, wann entsprechende Kontrollmaßnahmen stattfinden.
Moderne Software aus dem Bereich der „künstlichen Intelligenz“ basiert darauf, dass große Datenmengen ausgewertet werden. Dies schlägt sich in Betriebsvereinbarungen in Formulierungen wie dieser nieder:

„*Der Arbeitgeber ist befugt, die anfallenden Verhaltens- und Leistungsdaten mit dem Ziel der Optimierung seiner Systeme auszuwerten oder auswerten zu lassen. Eine Kontrolle von Leistung oder Verhalten verbindet sich hiermit nicht.*“

Eine solche weitgehende Verarbeitungsbefugnis steht im Widerspruch zum Grundsatz der Datenminimierung in Art. 5 Abs. 1 Buchstabe c) DSGVO. Hiernach müssen personenbezogene Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Gemeint ist damit nicht das verständliche Bestreben der Systemoptimierung, sondern der mit der Verarbeitung ursprünglich verfolgte Zweck. Zudem muss sich der Arbeitge-

ber in diesem Fall entgegenhalten lassen, dass er sein Ziel auch mit anonymisierten oder pseudonymisierten Daten erreichen könnte.
Konzepte zur regelmäßigen Datenlöschung sind vielen IT-Systemen bisher noch ebenso fremd wie solche zur Datenminimierung. Dies schlägt sich in Formulierungen nieder wie dieser:

„Beschäftigtendaten, die nicht mehr benötigt werden, sollen entsprechend der bestehenden technischen Möglichkeiten regelmäßig gelöscht werden. Eine Löschung soll spätestens nach zehn Jahren erfolgen. Ist dies technisch nicht möglich, sind die Daten für unzulässige Verwendungen zu sperren.“

Diese Formulierung steht im Widerspruch zum Grundsatz der Speicherbegrenzung in Art. 5 Abs. 1 Buchstabe e) DSGVO, nach dem personenbezogene Daten in einer Form gespeichert werden müssen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie dies für die ursprünglichen Verarbeitungszwecke erforderlich ist. Eine ersatzweise Sperrung sieht dieser Grundsatz ebenso wenig vor wie das pauschale Vorgeben einer (sehr langen) Regelspeicherfrist. Diese Formulierung steht zudem im Widerspruch zu dem schon mehrfach angesprochenen Grundsatz der Datenminierung.

2 Prüfraster für Betriebsvereinbarungen

– In bestehenden Betriebsvereinbarungen sowie in neu abzuschließenden müssen die in der DSGVO und im BDSG enthaltenen datenschutzrechtlichen Vorgaben umfassend berücksichtigt werden.
– Verweisen bereits abgeschlossene Betriebsvereinbarungen auf bestimmte Datenvorschriften (insbesondere solche des „alten“ BDSG), müssen diese durch Verweise auf die entsprechenden neuen Vorschriften in der DSGVO oder im BDSG ersetzt werden. Dabei sollte geprüft werden, ob sich der Regelungsgehalt der neuen Vorschriften verändert hat. Ist dies der Fall, muss ggf. über den Inhalt einer Betriebsvereinbarung neu verhandelt werden. Bis dahin gilt die vorherige Vorschrift weiter, es sei denn, sie steht im Widerspruch zum neuen Recht.
  Entsprechendes gilt, wenn Betriebsvereinbarungen dynamische Verweise auf das abgelöste Datenschutzrecht enthalten (etwa „*es gilt das BDSG in seiner aktuellen Fassung*“). In diesen Fällen kommt das neue Datenschutzrecht uneingeschränkt zur Anwendung, auch wenn sich hieraus Widersprüche zu Regelungen in der Betriebsvereinbarung ergeben. Lösen lassen sich diese ebenfalls nur durch eine Neufassung der Betriebsvereinbarung.
– Stehen Einzelregelungen in kollektivrechtlichen Vereinbarungen im Widerspruch zu zwingenden datenschutzrechtlichen Vorgaben (etwa weil statt einer gesetzlich vorgeschriebenen „Löschung“ nur eine „Sperrung“ von Daten vorgeschrieben ist oder weil Löschfristen vollständig fehlen), haben die gesetzlichen Vorgaben im Zweifel Vorrang.

– Lässt sich eine Regelung in einer Betriebsvereinbarung, die die alleinige Rechtsgrundlage für die Verwendung von Beschäftigtendaten ist, mit dem neuen Datenschutzrecht nicht mehr vereinbaren, steht dies der weiteren Verarbeitung dieser Informationen durch den Arbeitgeber entgegen. Dies folgt aus Art. 6 Abs. 1 DSGVO, der die Rechtmäßigkeit der Datenverarbeitung an das Vorliegen eines der dort genannten Erlaubnistatbestände knüpft. Bezogen auf Beschäftigungsverhältnisse präzisiert § 26 BDSG den Rahmen des Zulässigen und lässt durch seinen Abs. 4 die Ausgestaltung des Beschäftigtendatenschutzes durch Kollektivvereinbarungen ausdrücklich zu. Allerdings müssen sich entsprechende kollektivrechtliche Regelungen in dem durch die DSGVO vorgegebenen Rahmen bewegen.
– Sind kollektivrechtliche Erlaubnistatbestände gemessen an den neuen datenschutzrechtlichen Vorgaben unwirksam, muss überprüft werden, ob die entsprechende Betriebsvereinbarung auch ohne sie funktioniert. Das kann beispielsweise der Fall sein, wenn die Verarbeitung von Beschäftigtendaten in einem Personalinformationssystem grundsätzlich nach § 26 Abs. 1 Satz 1 BDSG erforderlich ist, nicht aber die in einer Betriebsvereinbarung geregelte Übermittlung von personenbezogenen Daten an ein anderes Konzernunternehmen. In diesem Fall muss lediglich die Übermittlung beendet werden, nicht aber die übrige (interne) Verarbeitung. Etwas anderes gilt, wenn die gesamte Verarbeitung ohne die kollektivrechtliche Übermittlungserlaubnis nicht mehr sinnvoll durchführbar ist. Sind die datenschutzwidrigen Erlaubnistatbestände in einer Betriebsvereinbarung die einzigen datenschutzrechtlichen Erlaubnisnormen, muss die hierauf basierende Verarbeitung unterbleiben.
– Folge des Fehlens einer kollektivrechtlichen Grundlage für die Verarbeitung von Beschäftigtendaten kann die Verhängung einer Geldbuße gegen den Arbeitgeber als datenschutzrechtlichen Verantwortlichen sein. Auf der Grundlage von Art. 83 Abs. 1 DSGVO zu verhängenden Geldbußen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Mit Blick auf das damit bestehende hohe finanzielle Risiko von bis zu zwanzig Millionen Euro oder von bis zu vier Prozent des Konzernjahresumsatzes des Vorjahres haben Arbeitgeber nunmehr ein großes Interesse daran, durch Kollektivvereinbarungen belastbare Rechtsgrundlagen zu schaffen. Aber auch Betriebsräte haben ein Interesse, die Verarbeitung von Beschäftigtendaten auf der kollektivrechtlichen Ebene so auszugestalten, dass die notwendige Rechtskonformität durchgängig gegeben ist.

2.1 Gibt es für die Verarbeitung von Beschäftigtendaten durch Arbeitgeber in Betriebsvereinbarungen relevante datenschutzrechtliche Erlaubnistatbestände?

– Einschlägige Erlaubnistatbestände in Betriebsvereinbarungen sind Regelungen, die Verarbeitungen und deren Zwecke beschreiben wie beispielsweise

„*Die Verarbeitung von Beschäftigtendaten mit dem System xy ist für alle Zwecke der Personalverwaltung zulässig.*“

Die Allgemeinheit dieser Formulierung kollidiert allerdings mit dem in Art. 5 Abs. 1 Buchstabe b) DSGVO verankerten Grundsatz der Zweckbindung und ist in dieser Allgemeinheit nicht datenschutzkonform. Erforderlich ist vielmehr eine konkrete Benennung der gewollten Zwecke wie etwa

„*Das System dient der Führung einer elektronischen Personalakte, in der alle Informationen über Beschäftigte zentral gespeichert werden. Die Verarbeitung dieser Daten ist nur zulässig, soweit dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.*“

2.2 Sind kollektivrechtliche Erlaubnistatbestände für die Verarbeitungen von Beschäftigtendaten hinreichend bestimmt?

– Vermieden werden müssen pauschale oder allgemeine Erlaubnistatbestände wie beispielsweise

„*Diese Vereinbarung ist im Unternehmen Rechtsgrundlage für die Verarbeitung der Beschäftigtendaten nach Art. 88 i.V.m. §26 BDSG n.F. sowie für die Verarbeitungen zur Wahrung berechtigter Interessen des Unternehmens nach Art. 6 Abs. 1 Buchstabe f) DSGVO*“

oder

„*Die personenbezogenen Daten der Beschäftigten dürfen für die jeweils vorgesehenen Zwecke verarbeitet werden. Weitergehende Verarbeitungszwecke sind unter Einhaltung des Art. 6 DSGVO zulässig.*“

Derartige allgemein gefasste Erlaubnistatbestände stehen im Widerspruch zu den in Art. 5 Abs. 1 Buchstabe b) DSGVO verankert Forderungen nach einer engen Zweckbestimmung der Datenverarbeitung. Sie schwächen zugleich den durch die DSGVO und das BDSG geschaffenen Schutz der Beschäftigten und reduzieren weiterhin die gesetzlichen Einwirkungs- und Kontrollmöglichkeiten von Betriebsräten in unangemessener Weise.

– Die notwendige datenschutzrechtlich Klarheit lässt sich durch Formulierungen erreichen wie

„Mit dem System dürfen Beschäftigtendaten ausschließlich für Zwecke der Arbeitszeiterfassung und der sich hieraus ableitenden Gehaltsabrechnung verarbeitet werden.“

2.3 Ist außerhalb der durch § 26 Abs. 1 Satz 1 BDSG bestimmten Erforderlichkeit eine Verarbeitung von Beschäftigtendaten zur Wahrung berechtigter Interessen des Arbeitgebers oder eines Dritten zulässig?

– Die Regelungen zum Beschäftigtendatenschutz in Art. 88 DSGVO und in § 26 BDSG begrenzen die Möglichkeiten von Arbeitgebern auf erforderliche Verarbeitungen von Beschäftigtendaten. Ist die Erforderlichkeit nicht gegeben, müssen Verarbeitungen unterbleiben. Dies gilt auch für die nach Art. 6 Abs. 1 Buchstabe f) DSGVO außerhalb eines Beschäftigungsverhältnisses mögliche Verarbeitung von personenbezogenen Daten zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten. Da es sich hierbei um Interessen handelt, die außerhalb der Erforderlichkeit des § 26 Abs. 1 Satz 1 BDSG angesiedelt sind, stehen einer solchen Verarbeitung immer überwiegende Interessen, Grundrechte und Grundfreiheiten der betroffenen Beschäftigten entgegen, die den Schutz personenbezogener Daten erfordern. Berechtigte Interessen von Arbeitgebern und von Dritten müssen hinter die durch die DSGVO geschützten Rechtspositionen der Beschäftigten zurücktreten. Klarstellend sollte hierzu in Betriebsvereinbarungen der Hinweis aufgenommen werden:

„Außerhalb der in § 26 BDSG bzw. der in dieser Betriebsvereinbarung genannten Erlaubnistatbestände ist die Verarbeitung von Beschäftigtendaten durch Arbeitgeber oder Dritte unzulässig.“

2.4 Muss eine Festlegung der Verarbeitungszwecke erfolgen?

– Nach dem Grundsatz in Art. 5 Abs. 1 Buchstabe b) DSGVO dürfen Beschäftigtendaten nur für festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden. Mit Blick auf die in Abs. 2 dieses Artikels enthaltenen Nachweispflichten führt dies dazu, dass Arbeitgeber in Vereinbarungen mit Beschäftigten bzw. im Rahmen von kollektivrechtlichen Regelungen entsprechende Festlegungen treffen müssen.

– Enthalten Betriebsvereinbarungen Aussagen zu Zwecken der Verarbeitungen, müssen diese abschließend und vollständig sein

„Zweck der Verarbeitung mit dem System xy ist die Erfassung, Prüfung, Verbuchung und Erstattung angefallener individueller Reisekosten.“

Datenschutzrechtlich nicht ausreichend sind im Regelfall hingegen pauschale und allgemeine Festlegungen wie

„Die Verarbeitung dient der Reisekostenabrechnung.“

2.5 Sind Änderungen eines einmal festgelegten Zwecks möglich?

– Art. 6 Abs. 4 DSGVO lässt Zweckänderungen unter den dort genannten Voraussetzungen grundsätzlich zu. Die Prüfung der Zulässigkeit von Zweckänderungen führt der Arbeitgeber durch. Zweckänderungen müssen sich allerdings im Rahmen der Erforderlichkeit gemäß § 26 Abs. 1 BDSG bewegen. Zu weitgehend wären allgemeine Formulierungen hierzu wie

„Zweckänderungen können erfolgen, wenn diese im betrieblichen Interesse sind.“

Eine derart allgemeine Formulierung spiegelt die Prüfanforderungen des Art. 6 Abs. 4 DSGVO nicht wieder. Mit Blick auf den bestehenden Spielraum, den Arbeitgeber haben, können Betriebsräte Festlegungen in Betriebsvereinbarungen zu einzelnen IT-Systemen dazu verlangen, das Zweckänderungen unterbleiben sollen.

„Die Verarbeitung ist nur zu den in dieser Betriebsvereinbarung festgelegten Zwecken zulässig. Zweckänderungen sind unzulässig.“

– Ist absehbar, dass sich Verarbeitungszwecke verändern können, sollte die Voraussetzungen hierfür festgeschrieben werden.

„Die Verarbeitung für andere Zwecke als den hier geregelten ist nur zulässig, wenn die Zweckänderung vorab mit dem zuständigen Betriebsrat vereinbart wurde und wenn sie sich im datenschutzrechtlich zulässigen Rahmen bewegt.“

2.6 Ist die Verarbeitung von sensiblen Daten, etwa zu Krankheiten oder zur Gewerkschaftszugehörigkeit, weiter zulässig?

– Die Verarbeitung sog. besonderer Kategorien personenbezogener Daten (hierzu gehören beispielsweise Informationen zur politischen Meinung, zur Gewerkschaftszugehörigkeit, zur Gesundheit, oder zur Sexualität) ist nach Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Deshalb sollte sich ein entsprechendes Verarbeitungsverbot in jeder Betriebsvereinbarung wiederfinden.
  Allerdings finden sich allgemeine Ausnahmen von diesem Verarbeitungsverbot in Art. 9 Abs. 2 DSGVO und spezifische Ausnahmen für Beschäftigungsverhältnisse in § 26 Abs. 3 BDSG. Diese Ausnahmen sollten durch Betriebsvereinbarungen auf die Fälle zwingender gesetzlicher Verpflichtungen zur Verarbeitung begrenzt werden.

  

  „Die Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten ist unzulässig. Ausgenommen von diesem Verbot sind gesetzlich zwingend vorgeschriebene Verarbeitungen dieser Daten sowie in dieser Betriebsvereinbarung ausdrücklich zugelassene Verarbeitungen für die hier genannten Zwecken.“

– Zu den ausdrücklich zugelassenen Zwecken können Verarbeitung der besonders geschützten Daten gehören, die dem Wohl der Beschäftigten dienen (etwa im Bereich des betrieblichen Eingliederungsmanagements). Derartige Ausnahmen müssen sich aber mit herausragenden Schutzmaßnahmen verbinden (etwa Verschlüsselung, begrenzte Zugriffsmöglichkeiten, kurze Löschfristen usw.).

2.7 Ist die Datenverarbeitung auf der Grundlage individueller Einwilligungen von Beschäftigten zulässig?

– Die Zulässigkeit der Verarbeitung personenbezogener Daten nennt Art. 6 Abs. 1 Buchstabe a) DSGVO ausdrücklich als Erlaubnistatbestand für die Datenverarbeitung. Die allgemeinen Voraussetzungen einer wirksamen Einwilligung sind in Art. 7 DSGVO aufgelistet. Für Beschäftigungsverhältnisse werden sie in § 26 Abs. 2 BDSG präzisiert.
  Die Einholung einer wirksamen Einwilligung setzt voraus, dass die Beschäftigten vor Abgabe einer Einwilligung auf die Freiwilligkeit ihrer Erklärung, auf die Möglichkeit einer Verweigerung der Einwilligung und die sich hiermit verbindenden Folgen sowie auf das bestehende Widerspruchsrecht hingewiesen werden. Darüber hinaus muss es ihnen auch tatsächlich möglich sein, eine erteilte Einwilligung jederzeit formlos, ohne Angabe von Gründen und ohne das Eintreten negativer Konsequenzen zu widerrufen.
– In einer Einwilligung müssen die zulässigen Verarbeitungszwecke mit Blick auf Art. 5 Abs. 1 Buchstabe b) DSGVO klar und abschließend

benannt werden. Diese Voraussetzung erfüllen pauschale Einwilligungen wie diese nicht:

„*Ich stimme der Verarbeitung meiner personenbezogenen Daten für betriebliche Zwecke zu.*“

Notwendig ist ein klarer Bezug zu einem festgelegten und abschließenden Zweck.

„*Ich stimmte der Verarbeitung meiner Reisekosten nebst der Erstellung der notwendigen Einzelabrechnungen durch den externen Dienstleister xy zu.*“

– Betriebsräte sollten bezogen auf verschiedene IT-Systeme Vereinbarungen anstreben, die individuelle Einwilligungen als Erlaubnistatbestände für die Verarbeitung nur in kollektivrechtlich ausdrücklich vereinbarten Fällen zulassen, etwa durch Formulierungen in IT-Rahmenvereinbarungen wie

„*Zur Wahrung der Rechte der Beschäftigten darf eine Verarbeitung ihrer Daten, die sich auf eine individuelle Einwilligung stützt, ausnahmsweise dann erfolgen, wenn der zuständige Betriebsrat bezogen auf einen konkreten Verarbeitungs- oder Regelungstatbestand der Einholung einer Einwilligung vorab zugestimmt hat.*“

2.8 Müssen Beschäftigte darüber informiert werden, wie ihre Daten durch den Arbeitgeber verarbeitet werden?

– Personenbezogene Daten müssen unter Beachtung des Grundsatzes der Transparenz in Art. 5 Abs. 1 Buchstabe a) DSGVO in einer für die Beschäftigten nachvollziehbaren Weise verarbeitet werden. Für sie muss deshalb stets erkennbar sein, welche Daten ihr Arbeitgeber für welche Zwecken verarbeitet.
In der Umsetzung dieses Transparenzgebots müssen Arbeitgeber als datenschutzrechtliche Verantwortliche sicherstellen, dass Beschäftigte die ihnen zustehenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form erhalten können und dass diese ihnen in einer klaren und einfachen Sprache übermittelt werden.
Nicht ausreichend zur Erreichung dieses Ziels sind allgemeine Regelungen in Betriebsvereinbarungen wie

„*Beschäftigte haben das Recht, Informationen dazu anzufordern, wie ihre Daten verarbeitet werden.*“

Zielführender sind aber Regelungen, die konkrete Informationspfade eröffnen wie

„Beschäftigte erhalten einmal jährlich eine allgemeine Information darüber, wo und für welche Zwecke ihre Daten im erforderlichen Umfang verarbeitet werden. Sie haben darüber jederzeit das Recht, detaillierte schriftliche Auskünfte zur Verarbeitung ihrer Daten zu erhalten. Ansprechpartner für Anfragen ist die Abteilung xy.“

– Eine gesetzeskonforme Information setzt neben der allgemeinverständlichen Vermittlung der Zwecke auch die Erläuterung der technischen Abläufe voraus. Entsprechende Informationen müssen ggf. in der jeweiligen Muttersprache der Beschäftigten erfolgen.

2.9 Muss / kann die Verarbeitung von Beschäftigtendaten begrenzt werden?

– Die Verarbeitung von Beschäftigtendaten muss nach den in Art. 5 Abs. 1 Buchstabe c) DSGVO enthaltenen Grundsatz der Datenminimierung dem Zweck angemessen und zugleich auf das notwendige Maß beschränkt sein. Dies steht einer pauschalen Erlaubnis zur Verarbeitung in einer Betriebsvereinbarung entgegen wie

„Die Verarbeitung erfolgt im Rahmen betrieblicher Notwendigkeiten und unter Beachtung wirtschaftlicher Notwendigkeiten und datenschutzrechtlicher Vorgaben.“

Derartige Formulierungen, die die Grenzen der Verarbeitung weitgehend in das Ermessen von Arbeitgebern stellen, sind mit Blick auf den Grundsatz der Datenminimierung zu weitgehend. Um diesem Grundsatz gerecht zu werden, müssen Arbeitgeber den Nachweis erbringen, dass die Verarbeitung bestimmter Beschäftigtendaten unumgänglich ist und auch nicht durch andere Maßnahmen ersetzt werden kann. Das Maß der notwendigen Verarbeitungen und deren Zwecke kann mit Blick auf die bestehenden Gestaltungsspielräume, die Arbeitgeber haben, in Betriebsvereinbarungen festgeschrieben werden:

„Die Verarbeitung von Beschäftigtendaten mit dem System xy erfolgt nur für die in dieser Vereinbarung genannten Zwecke. Diese Daten sind zu löschen, sobald der mit der Verarbeitung beabsichtigte Zweck erfüllt ist.“

– Bezogen auf erforderliche Beschäftigtendaten leitet sich aus dem Grundsatz der Datenminimierung technische Notwendigkeiten wie etwa die Pseudonymisierung oder die Verschlüsselung vorhandener Informationen ab. Entsprechende Vorgaben müssen in eine Betriebsvereinbarung aufgenommen werden.

„Soweit technisch möglich, sind die personenbezogenen Daten in verschlüsselter Form unter Einsatz anerkannter sicherer Verfahren zu verarbeiten. Weiterhin sind die Beschäftigtendaten nach Möglichkeit zu pseudonymisieren oder zu anonymisieren. Darüber hinaus sind diese Daten zu löschen, sobald der mit der Verarbeitung beabsichtigte Zweck erfüllt ist."

2.10 Müssen in Betriebsvereinbarungen Löschfristen festgelegt werden?

– Personenbezogene Daten dürfen nach dem Grundsatz der Speicherbegrenzung in Art. 5 Abs. 1 Buchstabe e) DSGVO nur so lange gespeichert werden, wie dies für die festgelegten Zwecke erforderlich ist. Deshalb müssen bezogen auf alle Beschäftigtendaten konkrete Löschfristen festgelegt werden, die so kurz wie möglich sind. Diese Vorgabe wird durch „offenen" Formulierungen wie

„*Beschäftigtendaten werden gelöscht, wenn sie für betriebliche Zwecke nicht mehr benötigt werden und wenn die Löschung technisch möglich ist.*"

oder

„*Alle Beschäftigtendaten werden nach zehn Jahren gelöscht, es sei denn, eine längere Speicherdauer ist aus rechtlichen Gründen notwendig.*"

nicht erfüllt.
Mit Blick auf die datenschutzrechtlichen Vorgaben zur Speicherbegrenzung, aber auch zur Datenminimierung, ist die Festschreibung möglichst kurzer Löschfristen in Betriebsvereinbarungen notwendig:

„*Die mit diesem System verarbeiteten Beschäftigtendaten werden spätestens drei Monate nach Abwicklung des jeweiligen Vorgangs gelöscht. Soweit Daten für Nachweiszwecke länger benötigt werden, erfolgt eine Pseudonymisierung der personenbezogenen Informationen. Die Liste mit den Klarnamen wird passwortgeschützt abgespeichert.*"

– Gibt es gesetzlich vorgeschriebene Mindestspeicherfristen (etwa im Bereich des Steuerrechts), müssen diese beachtet werden. Allerdings muss es sich hierbei um zwingende Fristen handeln. Diese können in Betriebsvereinbarungen durch Regelungen abgebildet werden wie

„*Leiten sich längere Speicherfristen aus zwingenden gesetzlichen Vorschriften ab, sind diese bei der Verarbeitung mit dem System xy zu beachten.*"

Zu unbestimmt sind hingegen Formulierungen wie

„*Gesetzliche oder vertragliche Speicherfristen sind zu beachten.*“

Aus derartig allgemeinen Festlegungen leitet sich keine wirksamen Speicherbegrenzungen ab.

2.11 Sind IT-Systeme aus dem Bereich der „Künstlichen Intelligenz“ datenschutzkonform, die systemübergreifend große Datenmengen ohne klare Zweckbindung verarbeiten und auszuwerten?

– Zwingende datenschutzrechtliche Grundsätze in Art. 5 Abs. 1 DSGVO wie die Zweckbindung der Verarbeitung oder die Datenminimierung stehen dem Vorhalten von Beschäftigtendaten zu unbestimmten Zwecken „auf Vorrat“ entgegen. Deshalb sind Formulierungen in Betriebsvereinbarungen, problematisch, die zweckfreie Vorratsdatenspeicherungen zulassen wie

„*Beschäftigtendaten können auch für andere Zwecke verarbeitet werden, solange hierbei Verhaltens- oder Leistungskontrollen ausgeschlossen sind.*“

– Ist die langfristigere Speicherung und Auswertung von Beschäftigtendaten aus nachvollziehbaren Gründen sinnvoll (etwa die Zahl von Wiederholungserkrankungen in bestimmten Arbeitsbereichen), können angestrebte Erkenntnisse im Regelfall durch anonymisierte oder pseudonymisierte Daten erreicht werden. In Betriebsvereinbarungen sollte dann aber sowohl die Art der entsprechenden Beschäftigtendaten als auch die Zwecke abschließend festgelegt werden:

„*Informationen über die individuelle Dauer einzelner Arbeitsvorgänge in der Produktion dürfen für Zwecke der Arbeitsoptimierung auch nach Wegfall des ursprünglichen Erhebungszwecks weiter verarbeitet werden. Voraussetzung ist allerdings, dass zu Beginn der Weiterverarbeitung eine Anonymisierung der Informationen erfolgt, die eine Identifikation einzelner Beschäftigter technisch und organisatorisch sicher ausschließt.*“

– Wird eine zweckfreie personenbezogene Vorratsdatenspeicherungen durch eine Betriebsvereinbarung legitimiert, müssen die Parteien bei der Ausgestaltung entsprechender Vereinbarungen allgemeine kollektivrechtliche Schutzvorschriften wie insbesondere § 75 Abs. 2 BetrVG beachten. Hiernach haben Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Damit sind Formen der Verarbeitung ausgeschlossen, die in unzulässiger Art und Weise in die Interessen, Grund-

rechte oder Grundfreiheiten von Beschäftigten eingreifen. Hierzu gehört beispielsweise eine Regelung, die die pauschale Verarbeitung aller in verschiedenen Systemen anfallenden Verhaltens- und Leistungsdaten durch „selbstlernende“ Systeme für übergreifende Zwecke wie etwa „Unternehmenssicherheit“ oder „Compliance“ erlaubt.

– Eine Vorratsdatenspeicherung der durch Art. 9 Abs. 1 DSGVO datenschutzrechtlich herausragend geschützten besonderen Kategorien personenbezogener Daten (vgl. hierzu auch Ziff. 6) ist für die Anbahnung, Durchführung oder Beendigung von Beschäftigungsverhältnissen grundsätzlich nicht erforderlich und sollte deshalb auch durch Betriebsvereinbarungen nicht zugelassen werden. Wird sie ausnahmsweise als sinnvoll erachtet (etwa die Erfassung von Wiederholungserkrankungen in bestimmten Bereichen für Zwecke des Arbeitsschutzes), muss zwingend festgelegt werden, dass Anonymisierungsverfahren zum Einsatz kommen.

„Informationen zu Wiederholungserkrankungen im Bereich xy dürfen für Zwecke der Gesundheitsvorsorge auch nach Wegfall des ursprünglichen Verarbeitungszwecks weiter vorgehalten und verarbeitet werden. Voraussetzung ist allerdings, dass zu Beginn dieser Verarbeitung eine Anonymisierung der Informationen über Erkrankungen erfolgt, die eine Identifikation einzelner Beschäftigter sicher ausschließt. Über die Art und Weise der Anonymisierung ist zwischen Arbeitgeber und Betriebsrat Einvernehmen herzustellen.“

2.12 Müssen die Schnittstellen festgelegt werden, über die eine Datenübertragung von und zu anderen Systemen erfolgt?

– Der Grundsatz der Transparenz in Art. 5 Abs. 1 Buchstabe a) DSGVO schreibt vor, dass personenbezogene Daten in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden. Die in Art. 5 Abs. 1 Buchstabe b) DSGVO folgenden Vorgaben zur Zweckbindung erlauben die Verarbeitung personenbezogener Daten nur für festgelegte, eindeutige und legitime Zwecke. Die Anwendung dieser Grundsätze auf Beschäftigtendaten und deren Verarbeitung in betrieblichen Systemen macht es notwendig, die Datenflüsse von einer zu mitbestimmungspflichtigen Anwendung zu anderen Systemen zu beschreiben und zu begrenzen. Allgemeine Formulierungen wie

„Im Rahmen der Erforderlichkeit oder aufgrund spezifischer betrieblicher Notwendigkeiten können Beschäftigtendaten zwischen dem hier geregelten System und anderen Systemen ausgetauscht werden.“

werden den Anforderungen nicht gerecht, die aus den Grundsätzen in Artikel 5 Abs. 1 DSGVO folgen.

– Bezogen auf einzelne IT-Anwendungen muss festgelegt werden, welche Schnittstellen es zu / von anderen IT-Anwendungen gibt und welche Daten über diese Schnittstellen empfangen oder versendet werden, etwa durch Formulierungen wie

„*Von dem hier geregelten System xy gibt es nur eine Schnittstelle zum System z. Über diese Schnittstelle wird aus dem System z nur die aktuelle Telefonnummer und die E-Mail-Adresse der Beschäftigten abgerufen.*“

– Um Betriebsvereinbarungen einfacher an sich ändernde technische Bedingungen anpassen zu können, kann die konkrete Festlegung der Schnittstellen und Datenflüsse ggf. auch in einer Anlage erfolgen.

„*Zulässige Schnittstellen von und zum System xy sind in einer Anlage zu dieser Betriebsvereinbarung aufgeführt. Die Anlage enthält jeweils auch Festlegungen dazu, welche Daten für welche Zwecke übermittelt werden.*“

Die in einer Betriebsvereinbarung in Bezug genommenen Anlagen müssen jeweils abschließend und vollständig sein (vgl. unter Ziff. 18).

– Gibt es Schnittstellen zu anderen Systemen, muss sichergestellt werden, dass diese ebenfalls kollektivrechtlich geregelt sind und dass die stattfindenden Übermittlungen datenschutzrechtlich zulässig sind.

„*Die Eröffnung von Schnittstellen zu anderen Systemen setzt voraus, dass auch diese kollektivrechtlich geregelt sind.*“

2.13 Ist die Vereinbarung eines Rollen- und Berechtigungskonzept notwendig?

– Der Zugriff auf personenbezogene Daten setzt das Vorliegen einer datenschutzrechtlichen Berechtigung voraus. Nur so lässt sich die in Art. 5 Abs. 1 Buchstabe a) DSGVO enthaltene Verpflichtung zur rechtmäßigen Verarbeitung umsetzen. Darüber hinaus gehört der Ausschluss des Zugriffs unberechtigter zu den allgemeinen Pflichten, die Verantwortlichen nach den Regelungen in den Art. 24 ff. DSGVO obliegen.
– Arbeitgeber müssen als Verantwortliche insbesondere sicherstellen, dass nur solche Personen und Stellen auf personenbezogene Daten zugreifen können, die hierfür eindeutig legitimiert sind. Die Festlegung berechtigter Zugriffe muss in umfassenden und vollständigen Rollen- und Berechtigungskonzepten erfolgen, die bezogen auf bestimmte Rollen die zulässigen Zugriffe und deren Zwecke auflisten. Auf diese können Betriebsvereinbarungen Bezug nehmen. Hierbei sind Formulierungen wie

„*die Zugriffsberechtigungen werden im jeweils aktuellen Rollen- und Berechtigungskonzept festgelegt*“

zu allgemein gehalten. Zudem kann ein Arbeitgeber in diesen Fällen aufgrund der statischen Formulierung das Rollen- und Berechtigungskonzept jeweils eigenständig verändern. Sinnvoller ist deshalb die Einbeziehung eines bestimmten Rollen- und Berechtigungskonzepts als Anlage einer Betriebsvereinbarung

„*Die Zugriffsberechtigungen zum System xy sind in einem Rollen- und Berechtigungskonzept festgelegt, dass dieser Betriebsvereinbarung als Anlage beigefügt ist.*“

2.14 Unter welchen Voraussetzungen können Beschäftigtendaten an andere Verantwortliche übermittelt werden?

– Art. 28 DSGVO sieht die Möglichkeit der Verarbeitung von personenbezogenen Daten im Auftrag des Verantwortlichen vor. Damit können auch Beschäftigtendaten im Auftrag eines Arbeitgebers durch Auftragsverarbeiter verarbeitet werden. Hierbei kann es sich sowohl um andere Konzernunternehmen handeln als auch durch andere Anbieter oder Unternehmen.
Unabhängig von der gesellschaftsrechtlichen oder vertraglichen Beziehung zum Arbeitgeber setzt die Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO voraus, dass personenbezogene Daten nur aufgrund dokumentierter Weisung des Verantwortlichen durchgeführt werden. Auf der Grundlage eines verbindlichen Vertrags zur Auftragserbringung müssen Gegenstand, Dauer, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt werden. Diese Vorgaben erfüllen allgemeine Regelungen in Betriebsvereinbarungen wie die folgende regelmäßig nicht.

„*Der Arbeitgeber ist im Rahmen datenschutzrechtlicher Vorgaben berechtigt, andere Konzernunternehmen oder Dritte mit der Verarbeitung von Beschäftigtendaten zu beauftragten.*“

Zielführender sind Vereinbarungen, die sicherstellen, dass entsprechende Verträge vorliegen und vom Betriebsrat geprüft werden, bevor eine Verarbeitung außerhalb des Betriebs erfolgen darf.

„*Die Vergabe von Aufträgen an Auftragsverarbeiter setzt voraus, dass die Rechte der Beschäftigten dabei umfassend gewahrt werden. Dies schließt die Beachtung aller einschlägigen Betriebsvereinbarungen durch Auftragsverarbeiter ein. Auch die nach dem BetrVG bestehenden Kontrollrechte des Betriebsrats müssen garantiert sein. Vor Aufnahme der Auftragsverarbeitung sind die Verträge mit den Auftragsverarbeitern dem Be-*

triebsrat zur Prüfung vorzulegen. Die Einführung der Auftragsverarbeitung setzt voraus, dass der Betriebsrat keine Nachteile für die Beschäftigten oder Einschränkungen seiner Mitwirkungs- und Mitbestimmungsrechte sieht.“

– Sollen Verarbeitungen erfolgen, die über eine Auftragsverarbeitung hinausgehen, bedürfen diese einer gesonderten Rechtsgrundlage in Form einer individuellen Einwilligung oder einer Kollektivvereinbarung. Ohne eine solche Rechtsgrundlage ist die Übermittlung von Beschäftigtendaten an Dritte (d.h. auch an andere Konzernunternehmen) unzulässig.

2.15 Müssen Fragen des technischen Datenschutzes bzw. der technischen Datensicherheit geregelt werden?

– Arbeitgeber sind als datenschutzrechtlich Verantwortliche nach den Art. 24 ff. DSGVO verpflichtet, alle notwendigen technischen und organisatorischen Schutzvorkehrungen zum Schutz der verarbeiteten personenbezogenen Daten sicherzustellen. Dabei müssen einschlägige datenschutzrechtliche Vorgaben wie insbesondere die Grundsätze in Art. 5 Abs. 1 DSGVO beachtet werden.
– In Betriebsvereinbarungen sollte der vom Arbeitgeber vorgesehene allgemein und für die geregelten IT-Systeme vorgesehene Schutzstandard festgeschrieben werden. Dabei ist eine Bezugnahme auf betriebliche Sicherheitskonzepte sinnvoll

„*Die Verarbeitung von Beschäftigtendaten erfolgt unter Berücksichtigung der Richtlinien zum technischen Datenschutz in der Fassung vom xx.xx.2019“, die dieser Betriebsvereinbarung als Anlage beigefügt ist.*“

Nicht empfehlenswert sind allgemeine Aussagen wie

„bei der Verarbeitung werden die aktuellen Sicherheitsvorgaben durch die IT-Abteilung eingehalten“

weil hierbei der Arbeitgeber bestehende Schutzstandards eigenständig ändern kann.
– Ist nach Art. 35 DSGVO eine Datenschutz-Folgenabschätzung vorgeschrieben, weil eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten von Beschäftigten zur Folge hat, müssen Arbeitgeber vor Aufnahme der Verarbeitung eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Werden im Rahmen dieser Datenschutz-Folgenabschätzung Risiken identifiziert, sollten die nach Art. 35 Abs. 7 Buchstabe d) DSGVO vorgeschriebenen Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren zum Schutz

personenbezogener Daten zum Gegenstand von Betriebsvereinbarungen gemacht werden.

„Um das festgestellte hohe Risiko der Verarbeitung mit dem System xy für die Rechte und Freiheiten der Beschäftigten auszuschließen bzw. zu minimieren, werden die folgenden Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren vereinbart: ….“

2.16 Haben Beschäftigte spezifische Datenschutzrechte?

– Die DSGVO räumt den von Datenverarbeitungen betroffenen Personen in den Art. 12 ff. zahlreiche Rechte ein. Hierzu gehören insbesondere die Informations- und Auskunftsansprüche in den Art. 12 bis 15 DSGVO, das Widerspruchsrecht in Art. 21 DSGSO, aber auch die neuen Rechte auf Löschung („Recht auf Vergessenwerden“) in Art. 17 DSGVO und auf Datenübertragbarkeit in Art. 20 DSGVO.
– Alle angesprochenen Rechte gelten uneingeschränkt auch für Beschäftigte. Zur konkreten Ausformung dieser Rechte gibt es eine umfangreiche Rechtsprechung der Arbeitsgerichte und des Bundesverfassungsgerichts, durch die die gegenseitigen Informationspflichten von Arbeitgebern und Beschäftigten präzisiert werden. Die bestehenden gesetzlichen Informationsrechte können nicht durch Formulierungen in Betriebsvereinbarungen eingeschränkt wie

„Der Arbeitgeber informiert die Beschäftigten bei Aufnahme der Verarbeitung in allgemeiner Form über die Zwecke des Systems.“

– Dem hohen Informationsanspruch der DSGVO werden Formulierungen gerecht wie

„Beschäftigte werden über die Zwecke der Verarbeitung vom Arbeitgeber in transparenter und verständlicher Form informiert. Die Information erfolgt bei Einführung des Systems und bei Änderungen der Verarbeitungszwecke. Beschäftigten bleibt es darüber hinaus unbenommen, ihre gesetzlichen Informations- und Auskunftsrechte wahrzunehmen. Entsprechende Anfragen werden vom Arbeitgeber unverzüglich beantwortet.“

2.17 Werden die gesetzlichen Rechte von Betriebsräten durch die neuen Datenschutzvorgaben beeinflusst?

– Betriebsräte gehören zum Betrieb und werden damit auch von der Definition des „Verantwortlichen“ i.S.v. Art. 4 Nr. 7 DSGVO erfasst. Durch § 26 Abs. 1 Satz 1 BDSG wird ausdrücklich klargestellt, dass die Verarbeitung von Beschäftigtendaten durch Betriebsräte zulässig ist, wenn sie zur Ausübung oder Erfüllung der sich aus einem Gesetz oder ei-

nem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.
Diese umfassende kollektivrechtliche Verarbeitungsbefugnis sollte nicht durch kollektivrechtliche Regelungen eingeschränkt werden wie beispielsweise

„der Betriebsrat kann die Einsicht in Protokolldateien des Systems xy nur verlangen, wenn er begründet darlegen kann, dass Verarbeitungen von Beschäftigtendaten mit diesem System im Widerspruch zu der Betriebsvereinbarungen stehen.“

Wichtig ist es, dass in Betriebsvereinbarungen unabhängig von hier getroffenen Regelungen immer festgehalten wird, dass

„dem Betriebsrat die Wahrnehmung seiner gesetzlichen Rechte im Übrigen unbenommen bleiben.“

2.18 Schlussbestimmung

Schlussbestimmungen von Betriebsvereinbarungen enthalten wichtige allgemeine Regelungen.

– Alle erwähnten Anlagen sind Bestandteil der Betriebsvereinbarung. Sie sind jeweils abschließend und vollständig. Anlagen können im Einvernehmen unabhängig von der Betriebsvereinbarung verändert werden.
– Die Betriebsvereinbarung tritt zum xx.xx.2019 in Kraft und kann mit einer Frist von …… Monaten gekündigt werden.
– Im Falle einer Kündigung wirkt die Betriebsvereinbarung insgesamt und einschließlich ihrer Anlagen bis zum Abschluss einer sie ersetzenden Vereinbarung nach.

3 Kollektivrechtliche Rahmenvereinbarungen

In vielen Betrieben und Unternehmen wird der Mitbestimmungsprozess bezüglich der IT-Anwendungen durch „IT-Rahmenvereinbarungen“ strukturiert und vereinfacht. Mit derartigen Vereinbarungen verbindet sich die Besonderheit, dass ihr Abschluss mangels eines einschlägigen Mitbestimmungstatbestands von den Betriebspartei erzwingbar ist, sondern nur einvernehmlich erfolgen kann. Diese Situation führt in der Praxis dazu, dass IT-Rahmenvereinbarungen das kollektivrechtlich vorgegebene Mitwirkungs- und Mitbestimmungsverfahren bezüglich der Einführung und Änderungen von technischen Einrichtungen nach § 87 Abs. 1 Nr. 6 BetrVG präzisieren, festlegen und teilweise auch modifizieren. Die Ausgestaltung derartiger Vereinbarungen muss, ebenso wie der von Betriebsvereinbarungen zu einzelnen IT-Systemen, den neuen datenschutzrechtlichen Vorgaben entsprechen.

Gleiches gilt für ebenfalls zu findende „Rahmenvereinbarungen zum Beschäftigtendatenschutz“, die den für alle angewendeten IT-Systeme zu beachtenden Datenschutzrahmen an einer Stelle einheitlich festlegen. Auch die hier getroffenen Regelungen müssen sich in dem datenschutzrechtlichen Rahmen bewegen, der durch die DSGVO und das BDSG vorgegeben wird.
Welcher Anpassungsbedarf bezogen auf die angesprochenen Rahmenvereinbarungen besteht, lässt sich in allgemeiner Form nur sehr schwer beantworten. Klärung bringt hier jeweils nur eine Einzelprüfung mit sich. Eine erste Orientierung ermöglicht das Prüfraster zu IT-Vereinbarungen in Abschnitt II, dass entsprechend auch auf „Rahmenvereinbarungen“ angewendet werden kann.
Unabhängig hiervon sollte sichergestellt werden, dass durch die verschiedenen Formen von Rahmenvereinbarungen keine pauschale Ausweitung von Verarbeitungsbefugnissen zugunsten von Arbeitgebern ermöglicht wird. Insoweit sollten auch in Rahmenvereinbarungen bereits in Abschnitt II.1 angesprochene Formulierungen vermieden werden wie

„*Diese Vereinbarung ist im Unternehmen Rechtsgrundlage für die Verarbeitung der Beschäftigtendaten nach Art. 88 i.V.m. §26 BDSG n.F. sowie für die Verarbeitungen zur Wahrung berechtigter Interessen des Unternehmens nach Art. 6 Abs. 1 Buchstabe f) DSGVO*“

oder

„*Die personenbezogenen Daten der Beschäftigten dürfen für die jeweils vorgesehenen Zwecke verarbeitet werden. Weitergehende Verarbeitungszwecke sind unter Einhaltung des Art. 6 DSGVO zulässig.*“

Vielmehr ist wie die Aufnahme der Formulierung

„*Diese Betriebsvereinbarung ist keine Erlaubnisgrundlage für die Verarbeitung von Beschäftigtendaten i.S.v. Art. 88 Abs. 1 DSGVO i.V.m. § 26 Abs. 4 BDSG. Etwas anderes gilt nur, wenn die Zulässigkeit bestimmter Verarbeitungen in dieser Betriebsvereinbarung für abschließend benannte Zwecke ausdrücklich vereinbart wird.*“

anzuraten.

Praxiswissen Betriebsvereinbarungen benötigt Euren Input!

Habt Ihr eine gute Vereinbarung rund um das Thema „Digitalisierung“ abgeschlossen? Anhand ausgewählter Betriebs- und Dienstvereinbarungen möchten wir aufzeigen, wie Mitbestimmungsakteure den digitalen Transformationsprozess mitgestalten. Macht mit und nehmt mit uns Kontakt auf! Wir freuen uns über Eure postalische oder elektronische Zusendung. Zitate werden nur in anonymisierter Form zugelassen. Nähere Informationen – www.boeckler.de/betriebsvereinbarungen

Mitbestimmung ist Zukunftsthema

Betriebsvereinbarungen zeigen, was betriebliche Praxis für die Ausgestaltung guter Arbeit leistet. Das I.M.U. der Hans-Böckler-Stiftung sammelt und dokumentiert Betriebs- und Dienstvereinbarungen zu allen Themen aus dem Alltag des Betriebs- und Personalrats. Aktuell konzentrieren wir uns auf Vereinbarungen, die rund um die digitale Transformation von Arbeit stehen.

Redaktion: Nils Werner, Hans-Böckler-Stiftung
Hans-Böckler-Straße 39, 40476 Düsseldorf

Kontakt: betriebsvereinbarung@boeckler.de

Online-Publikation, Download unter:
www.boeckler.de/betriebsvereinbarungen

[i] Aus Gründen der sprachlichen Vereinfachung ist im folgenden Text nur von „Betriebsvereinbarungen“ und von „Betriebsräten“ die Rede. Die Ausführungen gelten entsprechend aber auch für Dienstvereinbarungen und für Personalräte. Allerdings können sich bezogen auf Dienstvereinbarungen im Einzelfall Abweichungen aus anwendbaren landesrechtlichen Datenschutzvorschriften ableiten.