SCHWERPUNKT: GESETZGEBUNG ALS BETRIEBSGRUNDLAGE

Datenschutz durch Datenvermeidung und -sparsamkeit

Die neuen Regelungen im Bundesdatenschutzgesetz

Matthias Wilke / Eberhard Kiesche

HIER LESEN SIE:

- welche neuen Möglichkeiten Betriebs- und Personalräte durch die Novelle des Bundesdatenschutzgesetzes zum Beschäftigtendatenschutz haben
- wie eine Vereinbarung dazu beitragen kann, dass Datenvermeidung und -sparsamkeit die neue Leitlinie im Unternehmen wird
- wie die Interessenvertretung den Arbeitgeber zwingen kann, seine Datenverarbeitungssysteme rechtskonform auszugestalten

2001 wurde in das Bundesdatenschutzgesetz (BDSG) mit dem § 3a eine Vorschrift zur Datenvermeidung und -sparsamkeit eingeführt. Diese Vorschrift führte in der Praxis allerdings nur ein Schattendasein. Betriebsvereinbarungen verwiesen zwar darauf im Zusammenhang mit der Erforderlichkeit der Datenverarbeitung. Die praktische Umsetzung dieser Vorschrift machte aber erhebliche Probleme. Der zusätzliche Verweis in § 3a BDSG von 2001 auf den Einsatz von Anonymisierung und Pseudonymisierung hat ebenfalls kaum Wirksamkeit entfaltet. Das Mitführen der völligen Identität der Betroffenen in den Datenverarbeitungssystemen sollte dadurch reduziert werden. Es stellt sich aktuell die Frage, ob mit der vorliegenden BDSG-Novellierung die Situation für einen umfassenden Beschäftigtendatenschutz besser geworden ist und wie Interessenvertretungen die Umsetzung des neuen § 3a BDSG realisieren können. Im Folgenden werden die wesentlichen Neuerungen zur Datenvermeidung und -sparsamkeit dargestellt und deren Umsetzung am Beispiel von Kassensystemen erörtert.

Nach dem bisherigen § 3a BDSG hatten sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. In diesem Zusammenhang sollte insbesondere von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch gemacht werden, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Der Verstoß gegen die Vorschrift nach dem alten Recht war keine Ordnungswidrigkeit und damit nicht bußgeldbewehrt. Ein Verstoß gegen § 3a BDSG hatte zudem keine Rechtsfolge bei einer Kontrolle durch die Aufsichtsbehörde, deren Befugnisse weitgehend stumpf blieben und die die Umsetzung der Vorschrift nicht anordnen konnte.

Dies wurde von Vertretern von Datenschutzaufsichtsbehörden eingeräumt. Nur Betriebsräte konnten mit ihren Mitbestimmungsrechten versuchen, in einer Betriebsvereinbarung auf die Umsetzung dieser Vorschrift hinzuwirken. Durch die Festlegung in einer Vereinbarung, welche personenbezogenen Daten der Arbeitnehmer erhoben, verarbeitet und genutzt werden konnten und welche Zweckbindung dabei zu beachten war, konnte zumindest dem „Datenhunger" mancher Arbeitgeber gewisse Grenzen gesetzt werden. Dennoch kam es bei der Einführung von IT-Systemen oftmals vor, dass durch Betriebsvereinbarung quasi eine Vollerhebung von personenbezogenen Daten der Arbeitnehmer durch die technische Kontrolleinrichtung ermöglicht wurde und nur deren Auswertungs- und Verarbeitungsmöglichkeiten durch ein mitbestimmtes Berechtigungskonzept eingeschränkt wurden. Zumindest in der Präambel vieler IT-Vereinbarungen fand sich der Grundsatz der Datensparsamkeit und -vermeidung wieder, im eigentlichen Text blieb das dann aber ohne allzu weit reichende inhaltliche Konkretisierung.

Die geringe Wirksamkeit der Bestimmung zur Datenvermeidung und -sparsam-

keit in der Praxis wurde indirekt im § 11 Datenschutzauditgesetz-Entwurf[1] zugegeben. Dieser wurde allerdings 2009 wegen inhaltlicher Kritik zurückgezogen.

Das Datenschutzaudit-Gesetz soll jetzt erst in einem Pilotprojekt getestet werden. Unternehmen, die künftig ein Datenschutz-Gütesiegel erhalten wollen, sollten nach dem Auditgesetz-Entwurf zunächst nachweisen, dass sie die Datenschutzvorschriften nach dem BDSG umsetzen. Zusätzlich sollten sie die noch vom Datenschutzaudit-Ausschuss zu erlassenden Richtlinien zur Umsetzung des BDSG[2] einhalten. Die geplanten Richtlinien sollten sich auf die in der Praxis sichtbaren Schwachstellen bei der Umsetzung des Datenschutzes in Unternehmen beziehen. Eine Richtlinie sollte die betriebliche Umsetzung des § 3 a BDSG zum Thema haben.

§ 3 a BDSG neu formuliert

Der Gegenstandsbereich der Vorschrift zur Datenvermeidung und -sparsamkeit wird in der neuen Fassung 2009 präzisiert. Der Grundsatz der Datensparsamkeit, d. h. so wenig wie möglich personenbezogene Daten und der Grundsatz der Datenvermeidung, d. h. keine personenbezogene Daten, bezieht sich jetzt nicht nur auf die Auswahl und Gestaltung von Datenverarbeitungssystemen, sondern zusätzlich auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowohl innerhalb als auch außerhalb der automatisierten Datenverarbeitung.

Diese Änderungen hängen mit dem neuen § 32 Abs. 1 und 2 zum Beschäftigtendatenschutz in Verbindung mit § 28 Abs. 1 BDSG zusammen, der den Schutzbereich auf alle personenbezogenen Daten von Beschäftigten ausweitet, die zur Begründung, Durchführung und Beendigung eines Beschäftigungsverhältnisses erforderlich sind.

Anonymisierung und Pseudonymisierung

Auch in der neuen Fassung der Vorschrift wird herausgestellt, dass vor allem personenbezogene Daten dann zu anonymisieren oder zu pseudonymisieren sind, wenn es nach dem Verwendungszweck möglich ist und keinen im Verhältnis zum angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Bei Maßnahmen der Anonymisierung von personenbezogenen Daten ist eine Zuordnung von Einzelangaben zu einer bestimmten Person nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand möglich.[3] Bei Maßnahmen der Pseudonymisierung wird der Name oder andere Bestimmungsmerkmale durch ein Kennzeichen ersetzt und damit die Bestimmung des Betroffenen ausgeschlossen oder wesentlich erschwert.[4]

Erforderlichkeit der personenbezogenen Daten

Durch die Neuformulierungen in §§ 3 a und 32 BDSG wird der Grundsatz der Datenvermeidung und -sparsamkeit konkretisiert. Personenbezogene Daten der Beschäftigten gemäß § 3 Abs. 11 BDSG dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, aber nur dann, wenn sie für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für die Durchführung oder Beendigung erforderlich sind (§ 32 Satz 1 BDSG).

Vorher stand im § 28 Abs. 1 Nr. 1 BDSG die weichere Formulierung, dass die Daten dem Zweck des Arbeitsverhältnisses dienen mussten.[5] Zudem ist jetzt die Verarbeitung von Daten einbezogen. Bei der Umsetzung des neuen § 3 a BDSG heißt das im Hinblick auf § 32 BDSG, dass nunmehr ausdrücklich für jedes personenbezogene Datum der Beschäftigten im festzulegenden Datenkatalog als Anlage zur Betriebsvereinbarung die Erforderlichkeit abgeprüft werden muss. Diese ist vom Arbeitgeber nachzuweisen. Die Zielvorgabe der Datenvermeidung und -sparsamkeit hat sich in erster Linie an der Erforderlichkeit und Begrenztheit der Daten für einen berechtigten Zweck im Beschäftigungsverhältnis auszurichten.

AUS DEM BUNDESDATENSCHUTZGESETZ

§ 3 a BDSG – Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 32 BDSG – Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Neue Rechte für Aufsichtsbehörden

Leider ist festzustellen: Auch im novellierten BDSG ist ein Verstoß gegen § 3a keine Ordnungswidrigkeit. Die Bußgeldvorschriften insgesamt sind allerdings erweitert. In § 38 Abs. 5 sind aber die Befugnisse der Aufsichtsbehörden erheblich verschärft worden.

Ab sofort kann die Aufsichtsbehörde zur Gewährleistung dieses Gesetzes und anderer Vorschriften über den Datenschutz Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener oder technischer oder organisatorischer Mängel anordnen. Bei schweren Verstößen mit besonderen Gefährdungen des Persönlichkeitsrechts oder bei Nichtbefolgen von Anordnungen kann die Aufsichtsbehörde einzelne Verfahren oder die Erhebung, Verarbeitung und Nutzung personenbezogener Daten untersagen.

Frischer Wind für Arbeitnehmerdatenschutz

Für die Verarbeitung personenbezogener Daten der Beschäftigten in Unternehmen ist also § 32 BDSG der wesentliche Zulässigkeitstatbestand. Er ersetzt den § 28 Abs. 1 Nr. 1 BDSG als Rechtsgrundlage für die rechtmäßige Erhebung, Verarbeitung und Nutzung der Daten von Beschäftigten. Der neue § 28 Abs. 1 Nr. 1 BDSG findet für den Beschäftigtendatenschutz keine Anwendung mehr, § 28 Abs. 1 Nr. 2 BDSG bleibt als Rechtfertigung für die Verarbeitung von Beschäftigtendaten. § 32 erfasst jetzt alle Personen, die in einem Beschäftigungsverhältnis stehen.[6]

§ 32 Satz 1 BDSG legt zudem fest, dass bezogen auf alle Phasen eines Beschäftigungsverhältnisses bei der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten deren Erforderlichkeit und Zweckbindung zwingend sind.

Welche Daten der Arbeitgeber im Einzelnen konkret erheben, verarbeiten oder nutzen darf, kann auch § 32 BDSG nicht entnommen werden. Im Einzelfall muss nach wie vor die Verhältnismäßigkeit geprüft werden, also eine Abwägung zwischen den objektiven Informationsinteressen des Arbeitgebers mit dem Anspruch der Beschäftigten auf Persönlichkeitsschutz erfolgen.

Kontrolle von Daten zur Aufdeckung von Straftaten?

§ 32 Abs. 1 Satz 2 BDSG stellt zudem Anforderungen an den Datenschutz, wenn im Beschäftigungsverhältnis Straftaten wie Diebstahl oder Korruption aufgedeckt werden sollen. Dabei dürfen personenbezogene Daten der Betroffenen nur ausnahmsweise erhoben, verarbeitet oder genutzt werden, wenn ein konkreter Verdacht vorliegt und die Daten zur Aufdeckung der Straftat erforderlich sind. Der Arbeitgeber hat die Anhaltspunkte für den Verdacht schriftlich zu dokumentieren. Gleichzeitig muss geprüft werden, ob der Verwendung der Daten überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen und ob Art und Ausmaß der Erhebung, Verarbeitung und Nutzung der Daten im Hinblick auf den Anlass der Kontrolle noch verhältnismäßig ist. Es muss ein tatsächlich begründeter Verdacht da sein. Hier wird bereits deutlich: § 32 Abs. 1 Satz 2 BDSG kann nicht oder nur in geringem Maße für die Prävention von Straftaten oder Korruption als Rechtfertigung benutzt werden.[7] In § 32 Abs. 3 BDSG wird bestätigt, dass Mitbestimmungsrechte unberührt bleiben.

Kassensysteme für Kontrollen und Betrugsrecherche nutzen?

Was bedeuten die neuen BDSG-Vorschriften nun für IT-Regelungen in der Praxis für den Betriebsrat? Dies wird am Beispiel der Registrierkassen, die im Handel personenbezogene Daten der Beschäftigten zur Aufdeckung von Straftaten unbegrenzt sammeln, dargestellt.

Bei der Gestaltung von Betriebsvereinbarungen, nicht nur zu Kassensystemen, sollten die Betriebsräte die folgenden drei Prüfungsschritte vornehmen:

Für die Gestaltung von IT-gestützten Kassensystemen muss in einem *ersten Schritt* überprüft werden, ob sämtliche vom Arbeitgeber gewünschten Daten der Beschäftigten samt Auswertungen[8] für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses tatsächlich erforderlich sind. Eine Vollerhebung aller personenbezogenen Daten an der Kasse für den Zweck der kontinuierlichen Betrugsrecherche ist nach § 32 Abs. 1 Satz 1 BDSG offensichtlich nicht erforderlich, verletzt das Datenschutzprinzip der Transparenz[9] und ist zudem nicht verhältnismäßig.[10] Eine Vollerfassung und -überwachung von personenbezogenen Kassendaten ist allerdings schon nach dem alten § 28 Abs. 1 Nr. 1 BDSG eindeutig unzulässig und eine Verletzung des informationellen Selbstbestimmungsrechts der Beschäftigten gewesen.

In einem *zweiten Schritt* müssen die Zweckbestimmung der personenbezogenen Daten festgelegt und grundsätzlich Leistungs- und Verhaltenskontrollen ausgeschlossen werden.

Am Beispiel der Kassensysteme im Handel ist in einem *dritten Schritt* zu prüfen, ob alle von der Technik her möglichen Daten an den Kassen vom Arbeitgeber zur Aufdeckung von Inventurdifferenzen, Betrug und Unterschlagung rechtmäßig erhoben werden dürfen. Hierfür kann der § 32 Abs. 1 Satz 2 BDSG als Erlaubnistatbestand in Frage kommen.

Kontrolle/Datenhaltung mit Kassensystemen?

Schon allein die Erhebung aber auch die Verarbeitung und Nutzung derartiger Daten sind nach § 32 Satz 2 BDSG nur dann im Beschäftigungsverhältnis zulässig, wenn zu dokumentierende tatsächliche Anhaltspunkte den konkreten Verdacht begründen, dass der Betroffene bei der Arbeit eine Straftat begangen hat. Weiterhin wäre noch abzuwägen, ob die Erhebung, Verarbeitung und Nutzung von Daten zur Aufdeckung von Straftaten erforderlich ist, diese Datenverarbeitung noch verhältnismäßig im Hinblick auf den Anlass der Kontrolle ist und ob überwiegende schutzwürdige Interessen des Betroffenen gegeben sind.[11]

Die Prüfung ergibt: Präventiv dürfen nicht alle Beschäftigten an den Kassen mit dem Kassensystem jederzeit überwacht werden, da sie keinen Anlass für eine Vollkontrolle gegeben haben und diese zudem unverhältnismäßig wäre. Eine Vollkontrolle heißt: Alle Beschäftigten an der Kasse bleiben durch die Überwachungsmaßnahme nicht anonym, alle Aktivitäten am Kassenarbeitsplatz wie z. B. die eingescannten

Artikel pro Minute oder auch Stornos werden erfasst und alle überwachten Personen müssen immer mit arbeitsrechtlichen Maßnahmen wie z. B. Personalgesprächen mit der Kassenaufsicht, Versetzungen oder Herabgruppierungen rechnen. Diese sind gelebte Praxis in vielen Einzelhandelsunternehmen. Der Einsatz mancher Kassensysteme führt zur Erstellung von Persönlichkeitsprofilen und das ist nach BDSG und Grundgesetz nicht zulässig.[12] Es dürfen keine allwissenden Datenherren entstehen.[13] Hier liegt immer ein Verstoß gegen § 75 Abs. 2 BetrVG vor, weil eine freie Entfaltung der Persönlichkeit im Unternehmen nicht mehr möglich ist.

Eine Vorratsdatenhaltung von Kassendaten ist schon deshalb unzulässig, weil es an der Festlegung des Zwecks gemäß § 28 Abs. 1 Satz 2 BDSG fehlt. Zweckänderungen lassen sich nur bei Einsatz von konkreten Mitteln der Anonymisierung und Pseudonymisierung rechtfertigen.

Eine Verknüpfung von Kassendaten, die den Personalkauf erfassen, mit anderen personenbezogenen Daten der Beschäftigten an der Kasse, ist ebenfalls nicht zulässig.

Prüfung der Verhältnismäßigkeit

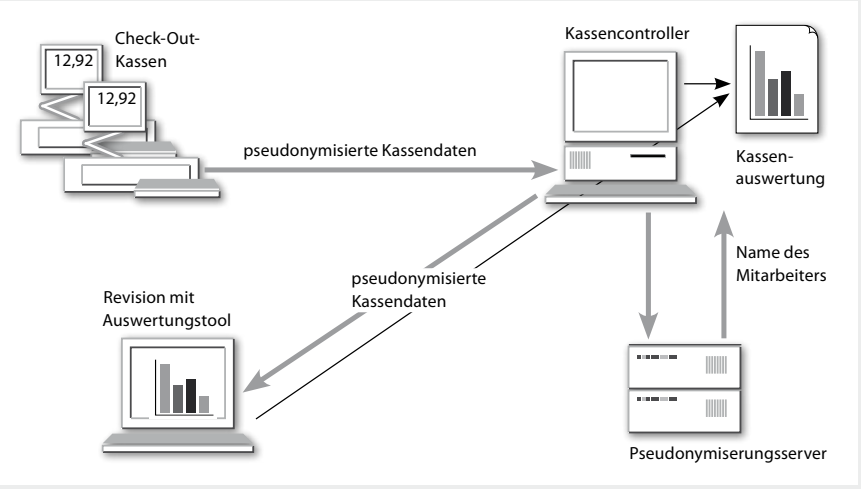
In analoger Anwendung der klaren Rechtsprechung des Bundesarbeitsgerichts (BAG) zur Videoüberwachung wird ebenfalls deutlich, dass eine dauerhafte Vollerfassung und Auswertung von Leistung und Verhalten der Beschäftigten an Kassen und der Einsatz verdeckter technischer Kontrolleinrichtungen ohne einen konkreten Anlass mit dem Persönlichkeitsschutz der Beschäftigten unvereinbar ist. Das BAG nimmt in seinem Beschluss vom 26. 8. 2008 ausgehend von Vorgaben des Bundesverfassungsgerichts eine umfassende Verhältnismäßigkeitsprüfung vor, die auf den Einsatz von Kassensystemen zu übertragen ist. Geheime Kontrollen sind grundsätzlich verboten und nur unter äußerst restriktiven Gesichtspunkten zulässig, wenn alle anderen Möglichkeiten ausscheiden.[14]

Vor einer Vollerfassung von personenbezogenen Daten der Beschäftigten an den Kassen wäre also immer noch zu überprüfen, ob nicht andere nichttechnische geeignete Mittel eingesetzt werden können um Kassenfehlbedienungen, Kassendiffe-

DIE PSEUDONYMISIERUNG AM BEISPIEL EINES KASSENSYSTEMS

Pseudonym (griechisch: „fälschlich so genannt"). Das Pseudonym ist ein fingierter Name, den besonders Künstler oder Schriftsteller aus unterschiedlichen Gründen verwenden. In Bezug auf Kassendaten bedeutet Pseudonymisierung, dass es keinen direkten Personenbezug mehr gibt.

Dafür erfolgt in der sogenannten Black-Box (Pseudonymisierungsserver) automatisiert eine Veränderung personenbezogener Daten (z. B. der Personalnummer) aufgrund einer Zuordnungsvorschrift (Algorithmus):



- Die Zuordnungsvorschrift und ihre Anwendung kann nur von drei Personen eingerichtet oder geändert werden.
- Der Name und das dazugehörige Pseudonym werden nirgendwo gespeichert.
- Die Umwandlung des Pseudonyms in den Namen des Kassenbedieners erfolgt nur bei konkretem Betrugsverdacht.
- Der Betriebsrat und der Hausleiter verfügen über jeweils eigene Passwörter um von der Filiale auf den Pseudonymisierungsserver in der Zentrale zugreifen zu können.
- Ergibt die Auswertung der (pseudonymisierten) Kassendaten, dass bei einem Benutzer auffällig viele Ereignisse (z.B. Stornos, Retoure, hohe Leergutauszahlung) auftreten, wird dies anhand von Unterlagen (Auswertungen der Kassenprotokolle) dokumentiert und der Betriebsrat darüber informiert. Der Hausleiter bzw. die Revision müssen weitere Verdachtspunkte mitteilen.
- Stimmt der Betriebsrat einer De-Pseudonymisierung zu, wird am Rechner (Kassencontroller) in der Filiale durch Eingabe der jeweiligen Passwörter durch den Filialleiter und den Betriebsrat mit dem Server (Black-Box) im Rechenzentrum eine Verbindung aufgebaut. Gemeinsam (Vier-Augen-Prinzip) wird das Pseudonym eingegeben, der Mitarbeitername wird aufgedeckt.
- Dem Mitarbeiter ist unmittelbar nach Feststellung, dass tatsächliche Anhaltspunkte auf einen Missbrauch vorliegen, darüber zu informieren, dass sein Pseudonym gelüftet wurde. Konnte der Betrugsverdacht ausgeräumt werden, wird für den Mitarbeiter ein neues Pseudonym generiert.
- Nach jeder De-Pseudonymisierung wird vom System automatisch ein fortlaufend nummeriertes Protokoll generiert, das dem zuständigen Betriebsrat unverzüglich übergeben wird um zu überprüfen, dass keine Aufdeckungen ohne Betriebsrat stattgefunden haben (z.B. durch „unbeabsichtigte" Kenntnis des Betriebsrats-Passworts).
- Stimmt der Betriebsrat der De-Pseudonymisierung nicht zu, findet keine Aufdeckung des Pseudonyms statt.

renzen und Kassenmanipulationen vorzubeugen. Das Mittel mit der geringsten Eingriffstiefe in das Persönlichkeitsrecht der Beschäftigten ist zu wählen. Hier bietet sich z. B. ein täglicher Kassensturz vor und nach der Kassentätigkeit an.

Ebenso scheidet für Handelsunternehmen eine gezielte Rasterfahndung nach bestimmten Kriterien aus, da in der Regel keine tatsächlich zu dokumentierenden Anhaltspunkte für eine Straftat vorhanden sind. Umfassende Bondatenanalyse zur Betrugsrecherche mit Programmen wie z. B. LossPrevention oder komplexe Data Mining-Verfahren[15] lassen sich mit den neuen Vorschriften des BDSG nicht rechtfertigen, weil nach § 28 Abs. 1 Nr. 2 BDSG schutzwürdige Interessen der Beschäftigten an der Kasse überwiegen.

Auch im Falle von Kassensystemen sind allenfalls stichprobenartige Kontrollen ohne Personenbezug eine geeignete Maßnahme zur Prävention von Kassenbetrug und Unterschlagung. Ergeben sich nach anonymisierten Datenerhebungen dann tatsächliche zu dokumentierende Anhaltspunkte für einen „begründeten Verdacht" auf eine schwere Straftat, sind vertiefende Kontrollen unter Einhaltung der Mitbestimmung des Betriebsrats und unter Hinzuziehung des Datenschutzbeauftragten möglich. Ein Verdacht auf einen Verstoß gegen betriebliche Anweisungen reicht nicht aus.[16]

Was bleibt den Unternehmen?

Die Verpflichtung in § 3 a BDSG, Datenvermeidung und -sparsamkeit durch Anonymisierung und Pseudonymisierung zu erreichen, zeigt nicht nur den Unternehmen im Handel einen gangbaren Weg auf. Sie müssen sich um die Art von Technik bemühen, die keine oder so wenig Daten mit Personenbezug wie möglich erhebt, verarbeitet oder nutzt. Es ist technisch in Kassensystemen ohne Probleme machbar, den Namen oder die Personalnummer wegzulassen und Auswertungen der Kassenjournals faktisch so zu anonymisieren, dass eine Zuordnung der Daten zu Beschäftigten in der Filiale nicht mehr möglich ist. Dann entfallen die Vorschriften des BDSG. Hierbei muss aber von Betriebsräten zusätzlich überprüft werden, ob ggf. weitere personenbeziehbare Daten im Betrieb vorhanden sind, die die gewünschte Anonymisierung wieder aufheben würde. In dem Fall ist in einem zweiten Schritt das Mittel der Pseudonymisierung zu benutzen.

Pseudonymisierung ein Weg für präventive Maßnahmen

Für den Zweck der Betrugsrecherche bietet sich zusätzlich noch der Weg an, hierfür erforderliche personenbezogene Daten an den Kassen zu erheben aber anschließend den Personenbezug durch Pseudonymisierung zu ersetzen.

Pseudonymisierung bedeutet, den Personenbezug im Kassenjournal durch ein Kennzeichen oder Alias zu ersetzen und damit die personenbezogenen Daten der Beschäftigten zu pseudonymisieren. Die Zuordnung von pseudonymisierten Benutzerkennzeichen und Namensliste z. B. bei Kassiererinnen erfolgt auf einer gesondert einzurichtenden Liste. Diese kann im Safe eines Treuhänders verwahrt bleiben und Einrichtung, Pflege und Zugriff auf die Pseudonyme nur nach dem Vier- oder Sechs-Augen-Prinzip gewährt werden. Wenn tatsächliche Anhaltspunkte für Betrug und Unterschlagung am Kassenarbeitsplatz vorliegen, die dokumentiert worden sind, kann in die Liste geschaut werden, wer tatsächlich an der Kasse zum betreffenden Zeitpunkt gesessen hat. Anschließend hat sofort eine Unterrichtung des Betroffenen zu erfolgen und ihm ist eine Gelegenheit zur Stellungnahme zu geben. Wird der Verdacht ausgeräumt, müssen unverzüglich alle personenbezogenen Kassendaten gelöscht werden.

Das novellierte BDSG zwingt also die Unternehmen viel stärker als bisher die vorhandenen technischen Möglichkeiten zur Anonymisierung und Pseudonymisierung zu nutzen. Gute Erfahrungen mit Pseudonymisierung sind vor allem im öffentlichen Dienst oder mit medizinischen Patientenakten gemacht worden. Der Aufwand für eine vorzunehmende Pseudonymisierung auch in Handelsunternehmen wird von Arbeitgebern überschätzt und ist keinesfalls unverhältnismäßig. Wenn zur Aufdeckung von Straftaten noch personenbezogene Kassendaten präventiv erhoben und nur im Falle von tatsächlichen Anhaltspunkten verarbeitet und genutzt werden sollen, brauchen Unternehmen jetzt auf jeden Fall das konkrete Mittel der Pseudonymisierung, das konkret aber nur über eine Betriebsvereinbarung als Erlaubnisvorschrift[17] zu verwirklichen ist. Ansonsten bleibt den Unternehmen für die Prävention nur das Mittel der anonymisierten stichprobenartigen Kontrollen.

Mitbestimmung und Betriebsvereinbarung

Interessenvertretungen können die neuen Vorschriften zum Beschäftigtendatenschutz nutzen und durch den Abschluss von Betriebsvereinbarungen mehr als bisher dazu beitragen, dass Datenvermeidung und -sparsamkeit die neue Leitmaxime der Unternehmen wird. Sie können nach § 87 Abs. 1 Nr. 6 BetrVG den Abschluss einer Betriebsvereinbarung z. B. zu Kassensystemen oder anderen technischen Kontrolleinrichtungen zur Mitarbeiterüberwachung erzwingen.[18] Betriebsräte können zudem bei IT-Systemen, die im Unternehmen zwar eingeführt aber bislang nicht geregelt sind, ebenfalls Betriebsvereinbarungen durchsetzen.

Eine Betriebsvereinbarung ist eine Rechtsvorschrift gemäß § 4 Abs. 1 BDSG und im unklaren Feld des Beschäftigtendatenschutzes den Unternehmen zur Erfüllung der datenschutzrechtlichen Anforderungen dringend zu empfehlen. Die Betriebsparteien können allerdings den Standard des neuen BDSG nicht unterschreiten, auch wenn sich dies Arbeitgeber jetzt verstärkt wünschen. Eine Schlechterstellung in der Betriebsvereinbarung gegenüber den Regelungen des neuen BDSG wäre ein eindeutiger Verstoß gegen das Persönlichkeitsrecht der Betroffenen und liegt nicht in der Regelungsbefugnis der Betriebsparteien. Das BDSG ist nicht abdingbar.[19]

Kommen Arbeitgeber den berechtigten Wünschen nach Anonymisierung und Pseudonymisierung nicht nach, kann der Betriebsrat die Verhandlungen für gescheitert erklären und für den Abschluss einer Betriebsvereinbarung die Einigungsstelle gemäß § 76 BetrVG einrichten lassen. Voraussetzung für eine rechtsverträgliche

Betriebsvereinbarung ist allerdings die umfassende Information durch den Arbeitgeber über die technischen Möglichkeiten der Datenverarbeitungssysteme.

Fazit

Betriebsräte haben nach § 80 Abs. 1 Nr. 1 BetrVG das Recht, die Einhaltung der zugunsten der Arbeitnehmer geltenden Gesetze und damit auch des BDSG zu überwachen und Informationen nach § 80 Abs. 2 BetrVG vom Arbeitgeber anzufordern, wie z. B. § 3 a und § 32 BDSG für Datenerhebungen, -verwendungen und –nutzungen umgesetzt werden sollen. Sie haben es in der Hand, die Arbeitgeber zu einer rechtskonformen Ausgestaltung ihrer Datenverarbeitungssysteme zu zwingen. Sie sollten ihre Arbeitgeber an die Datenschutzskandale der letzten Jahre erinnern und verdeutlichen, wie schnell Datenschutzskandale und -pannen einen Imageverlust der Unternehmen bewirken. Pseudonymisierung ist ein gangbarer und günstiger Weg um das informationelle Selbstbestimmungsrecht der Beschäftigten und berechtigte Interessen der Unternehmen, z. B. im Einzelhandel, in Einklang zu bringen. Notfalls können Betriebsräte Aufsichtsbehörden einschalten, die jetzt andere und bessere Sanktionsmittel haben. Die Aufsichtsbehörden sollten personell besser ausgestattet werden, damit sie die Umsetzung von BDSG-Vorschriften wie z. B. Datenvermeidung und -sparsamkeit tatsächlich kontrollieren können.

Autoren

Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel, info@dtb-kassel.de; **Dr. Eberhard Kiesche**, Arbeitnehmerorientierte Beratung (AoB), Bremen, eberhard.kiesche@t-online.de

Fußnoten

1 Vom September 2007 und 22. 10. 2008
2 Vgl. § 11 Abs. 1 Nr. 2 Entwurf Datenschutzauditgesetz
3 Vgl. § 3 Abs. 6 BDSG
4 Vgl. § 6 a BDSG
5 Vgl. Thüsing: Datenschutz im Arbeitsverhältnis, in: NZA 2009, 865 [866]
6 § 3 Abs. 11 BDSG
7 Vgl. Thüsing, a.a.O. 686
8 Beispiele: Artikel- und Warengruppendaten, Marktabrechnungsdaten, Aktionsmengencontrolling, Personalrabatteinkäufe und EC-Transaktionen
9 Anhang zur Bildschirmarbeitverordnung Nr. 20: Keine geheimen Kontrollen zulässig. In Einzelhandelsunternehmen werden die Beschäftigten über Kontrollmöglichkeiten der Kassensysteme faktisch in der Regel nicht unterrichtet
10 BAG, Beschluss vom 26. 8. 2008, Az.: 1 ABR 16/07, Rn. 17 und insbes. Rn. 26
11 Vgl. auch die Vorschrift in § 100 Abs. 3 Telekommunikationsgesetz (TKG)
12 Däubler: Ein Gesetz über den Arbeitnehmerdatenschutz, in: RDV 1999, 244 [248]
13 Däubler, in: Däubler/Klebe/Wedde/Weichert, Kommentar zum BDSG, 3. Aufl. im Erscheinen, § 32, Rn. 69
14 BAG, Beschluss vom 27. 3. 2003, NZA 2003, 1193 und BAG, Beschluss vom 26. 8. 2008, Az.: 1 ABR 16/07, NZA 2008, 1187, Rn. 21
15 Wilke: Data Mining – Rasterfahndung im Betrieb, in: AiB 2006, 155 ff.
16 Der Bundesverband Deutscher Arbeitgeberverbände (BDA) läuft Sturm gegen § 32 Satz 2 BDSG und will den gesamten § 32 BDSG wieder abschaffen lassen
17 § 4 Abs. 1 BDSG
18 Vgl. Grobys/Steinau-Steinrück, NJW-Spezial 12/2008, 403
19 Trittin/Fischer: Datenschutz und Mitbestimmung, in: NZA 2009, 343 [345]

BEISPIEL EINER BETRIEBSVEREINBARUNG

Zwischen der Geschäftsführung der Firma XYZ GmbH,

und dem Betriebsrat der Firma XYZ GmbH,

wird eine Betriebsvereinbarung über die Einführung, Anwendung und Weiterentwicklung des Kassensystems XXX und des Auswertungstools YYY vereinbart.

§ 1 – Zielsetzungen

Absicht dieser Betriebsvereinbarung ist sicherzustellen, dass

- eine effiziente Nutzung des Kassensystems XXX und des Auswertungssystems YYY zur Unterstützung der Ziele des Unternehmens gewährleistet ist,
- die Mitarbeiterinnen und Mitarbeiter[1] vor unzulässiger und unnötiger Nutzung der über sie erfassten und gespeicherten Daten geschützt werden und
- das informationelle Selbstbestimmungsrecht der Mitarbeiterinnen und Mitarbeiter gewahrt wird.

§ 2 – Zweckbindung

Die Anwendung des Kassensystems XXX und des Auswertungstools YYY dient folgenden Zwecken:

- Organisation des reibungslosen betriebswirtschaftlichen Ablaufs:
  - Umsatzerfassung von Artikel- und Warengruppendaten,
  - Marktabrechnungsdaten,
  - Aktionsmengencontrolling;
- Management von Personalrabatteinkäufen und EC-Transaktionen;
- Unterstützung des Qualitätsmanagements;
- Schutz der Firma XYZ GmbH vor Vermögensverlusten;
- Identifizierung von Schwachstellen in Hard- und Software;
- Aufdeckung von Schwachstellen organisatorischer Art;
- Aufdeckung von Inventurdifferenzen aufgrund von unabsichtlichen Kassenfehlbedienungen und
- Betrugsrecherche und Nachweis von Unterschlagungen.

§ 3 – Gegenstand, Geltungsbereich und Grundsätze

Diese Betriebsvereinbarung gilt für die Einführung, den Einsatz, die Anwendung, Änderung, Erweiterung und Weiterentwicklung des Kassensystems XXX und des Auswertungstools YYY.

Die Betriebsvereinbarung gilt für alle Beschäftigten der Firma XYZ GmbH einschließlich der Aushilfen und der beschäftigten Leiharbeitnehmer.

Eine Verknüpfung der Kassensystem-Daten der Beschäftigten zum Zweck der Erstellung von Persönlichkeitsprofilen ist nicht zulässig.

1 Im Folgenden wird aufgrund der besseren Lesbarkeit auf die weibliche Form verzichtet. Die Formulierung „Arbeitnehmer, Beschäftigter oder Mitarbeiter" schließt jeweils die weibliche Form mit ein.

§ 4 – Systemdokumentation

Das eingesetzte Kassensystem XXX, das Auswertungstool YYY und die Vernetzung werden abschließend in Anlage ## dokumentiert. Hierzu gehören die Hardware, die Hardwarekonfiguration, der Datenflussplan und die eingesetzten Programme. In Anlage ## wird die eingesetzte Software abschließend dokumentiert.

Berichte und Auswertungen des Kassensystems XXX und des Auswertungstools YYY werden in Anlage ## samt Empfängerkreis und Löschfristen vereinbart und festgeschrieben.

Die Anlagen sind Bestandteil dieser Betriebsvereinbarung.

§ 5 – Leistungs- und Verhaltenskontrollen

Die Erhebung, Verarbeitung, Nutzung, Speicherung oder Veränderung des Kassensystems XXX und des Auswertungstools YYY zu Leistungs- und Verhaltenskontrollen ist unzulässig.

Fehler und Mängel bei der Benutzung der Kassen bzw. bei der Leistungserbringung der Kassenbediener, die in den Qualitätsmanagement-Berichtsdaten offenkundig werden, dürfen nicht personenbezogen oder –beziehbar verarbeitet oder genutzt werden.

Schulungsmaßnahmen aufgrund von festgestellten Qualitätsmängeln sind ausschließlich für die jeweilige Filiale insgesamt durchzuführen.

Fehlbedienungsauswertungen sind nur dann zulässig, wenn sie sich auf eine Grundgesamtheit von mindestens acht Personen beziehen.

§ 6 – Datenvermeidung

Bei der Erhebung von personenbezogenen Daten der Beschäftigten an den Kassen ist § 3a BDSG zu beachten. Datenvermeidung und -sparsamkeit sind für die Anwendung des Kassensystems XXX und des Auswertungstools YYY durch konkrete Maßnahmen der Anonymisierung und Pseudonymisierung sichergestellt.

Vor dem Einsatz umfassender Auswertungen, Reports und Statistiken mit Hilfe des Kassensystems XXX und des Auswertungstools YYY ist zu prüfen, mit welchen anderen auch nichttechnischen Mitteln Kassenfehlbedienungen, -differenzen und -manipulationen vorgebeugt werden können. Es ist ein täglicher Kassensturz vorher und nachher vorzunehmen. Jährlich ist dem Betriebsrat eine Bedarfsermittlung vorzulegen, die aufzeigt, welche Kassendifferenzen, -manipulationen und -probleme in der Vergangenheit aufgetreten sind und ob der Einsatz eines computergestützten Kassenanalysesystems erforderlich im Sinne des § 32 Abs. 1 Satz 1 und 2 BDSG ist.

Die Kassendaten sind grundsätzlich so zu anonymisieren, dass eine faktische Zuordnung der erfassten Daten zu Personen in der Filiale nicht mehr möglich ist.

Wird nachgewiesen, dass eine Zuordnung zu Benutzern in der Filiale möglich sein muss, ist eine Pseudonymisierung vorzunehmen.

§ 7 – Pseudonymisierung

Jeder Benutzer des Kassensystems XXX erhält zur Anmeldung und Berechtigungsprüfung am System eine Codekarte mit einer pseudonymisierten Benutzerkennung.

Die Codekarte mit der pseudonymisierten Benutzerkennung wird zentral erstellt. Die Zuordnungsregel zur Generierung des Pseudonyms erfolgt mit einer eigenen Hardwarekomponente mit zugehöriger Software als Black-Box-Lösung (Pseudonymisierungsserver), die in der Anlage ## beschrieben ist.

Die Einrichtung, die Pflege und der Zugriff auf die Zuordnungsregel zur Generierung der Benutzerkennung geschieht nach dem Sechs-Augen-Prinzip. Berechtigt sind dazu gemeinsam der Datenschutzbeauftragte, der System-Administrator und der Betriebsrat.

Die Benutzerkennung und der Name sind im System nicht hinterlegt und fest zugeordnet.

§ 8 – De-Pseudonymisierung

Die Aufhebung der Pseudonymisierung (De-Pseudonymisierung) wird nur zur Aufklärung strafbarer Handlungen und zur Unterstützung hierfür gerechtfertigter betriebsinterner Ermittlungen vorgenommen. Grundlage hierfür sind folgende Anlässe:

- Dringender, begründeter und dokumentierter Verdacht auf Betrug oder Unterschlagung am Kassenarbeitsplatz und
- Hinweise Dritter zu Unregelmäßigkeiten, die den Verdacht auf strafbare Handlungen am Kassenarbeitsplatz rechtfertigen.

Anhaltspunkte und Hinweise sind zu dokumentieren.

Der Hausleiter oder sein Vertreter teilt dem zuständigen Betriebsrat unter Verpflichtung zur Verschwiegenheit anhand von Unterlagen die Gründe für die De-Pseudonymisierung mit.

Erhebt der Betriebsrat gegen die De-Pseudonymisierung nach Abwägung aller Vorgaben in § 32 Abs. 1 Satz 2 BDSG keine Einwände, kommt es zur kontrollierten Offenlegung und Freigabe der Identität des Mitarbeiters am Kassenarbeitsplatz.

Die Aufhebung des Pseudonyms erfolgt nach dem Vier-Augen-Prinzip. Das Verfahren ist in Anlage ## festgeschrieben.

Sobald der Personenbezug hergestellt ist und der Name des Beschäftigten vorliegt, muss bei Speicherung, Verarbeitung und Nutzung dieser personenbezogenen Daten der betroffene Beschäftigte unverzüglich benachrichtigt werden. Ihm ist das Recht auf eine Stellungnahme einzuräumen. Er kann auf Wunsch ein Mitglied des Betriebsrats hinzuziehen.

Die Speicherung, Nutzung und Verarbeitung der erhobenen Kassendaten durch die Firma XYZ GmbH ist ausschließlich für eventuelle Gerichtsverfahren zulässig. Wird der Anfangsverdacht ausgeräumt, müssen unverzüglich alle diesbezüglichen personenbezogenen Daten der betroffenen Beschäftigten gelöscht werden.

Nach jeder De-Pseudonymisierung wird vom System automatisch ein fortlaufend nummeriertes Protokoll generiert, das dem zuständigen Betriebsrat unverzüglich übergeben wird.

§ 9 – Datenschutz und Berechtigungskonzept

Das Berechtigungskonzept für die Nutzung des Kassensystems XXX und des Auswertungstools YYY wird zwischen Geschäftsführung und Betriebsrat vereinbart und ist als Anlage ## Bestandteil dieser Betriebsvereinbarung.

Zugriffe auf die Daten und Auswertungen haben nur Mitarbeiter der Revision/Sicherheitsabteilung und die IT-Systemadministratoren der Firma XXX GmbH im Rahmen der Auftragsdatenverarbeitung. Es muss sowohl technisch wie organisatorisch gemäß § 9 BDSG sichergestellt werden, dass ausschließlich die berechtigten Personen Zugang zu den Daten erhalten.

§ 10 – Löschfristen

Die Daten des Kassensystems XXX und des Auswertungstools YYY sind spätestens nach ___ Tagen zu löschen.

§ 11 – Rechte der Beschäftigten

Alle Beschäftigten werden über den Einsatz und die Möglichkeiten des Kassensystems XXX und des Auswertungstools YYY schriftlich informiert. Der Erhalt der Information durch den Mitarbeiter ist schriftlich zu dokumentieren. Die Information erfolgt in verständlicher Weise über alle wesentlichen Funktionalitäten und Auswirkungen des Kassensystems und über die bei der Firma XYZ GmbH vorgenommenen Pseudonymisierungen und Anonymisierungen.

Die Geschäftsführung stellt sicher, dass alle neu eingestellten Beschäftigten, die an Kassenarbeitsplätzen eingesetzt werden, vor Beginn ihrer Tätigkeit schriftlich über das Kassensystem XXX und das Auswertungstool YYY informiert werden. Die Beschäftigten sind im Rahmen der Unterweisung an den Kassensystemen auch auf deren Einsatz und die Wirkungsweise zu belehren.

Die Rechte der Beschäftigten auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung nach §§ 33 – 35 BDSG bleiben unberührt.

§ 12 – Beweisverwertungsverbot

Informationen, die unter Verletzung der Bestimmungen dieser Betriebsvereinbarung gewonnen werden, dürfen nicht verwendet werden. Auf diesen Informationen basierende arbeitsrechtliche Maßnahmen sind unwirksam.

Werden Fehler bei der Bedienung der Kasse infolge der De-Pseudonymisierung personenbezogen oder -beziehbar gemacht, dürfen die festgestellten Fehler nicht zu Leistungskontrollen und arbeitsrechtlichen Sanktionen genutzt werden.

§ 13 – Technisch-organisatorische Maßnahmen des Datenschutzes

Die Geschäftsführung der Firma XYZ GmbH gewährleistet, dass die Daten der Beschäftigten umfassend gegen Missbrauch geschützt werden. Das Datenschutzkonzept zum Kassensystem und dem Auswertungstool gemäß § 9 und Anlage zu § 9 BDSG ist Bestandteil dieser Betriebsvereinbarung (Anlage ##).

Der betriebliche Datenschutzbeauftragte (_____) informiert jährlich den Betriebsrat über neue Methoden und Erkenntnisse zur Anonymisierung und Pseudonymisierung.

Alle Benutzeraktivitäten des Kassencontrollers und des Pseudonymisierungsservers werden protokolliert.

Auf Wunsch werden dem Betriebsrat die Protokolle zur Verfügung gestellt und erläutert.

Mitarbeiter der Firma XXX GmbH als Auftragnehmer, IT-Systemadministratoren, Marktleiter und Mitarbeiter der Revision werden auf die Einhaltung des Datenschutzes gemäß § 5 BDSG verpflichtet.

§ 14 – Mitbestimmung des Betriebsrats

Über Änderungen und Erweiterungen des Kassensystems XXX und des Auswertungstools YYY wird der Betriebsrat der Firma XYZ GmbH rechtzeitig und umfassend anhand von Unterlagen nach § 80 Abs. 2 BetrVG informiert.

Änderungen und Erweiterungen der Systeme sind mitbestimmungspflichtig. Hierzu gehören insbesondere Änderungen und Erweiterungen der Hard- und Software, Ausweitungen des Datenkatalogs und der Auswertungen, Änderungen des Zugriffsberechtigungs- und des Datenschutzkonzepts nach § 9 BDSG sowie der Zweckbestimmung des Systems.

Die Firma XYZ GmbH stellt sicher, dass bei der Auftragsdatenverarbeitung durch den Auftragnehmer Firma XXX GmbH der Betriebsrat seine Überwachungsaufgabe gemäß § 80 Abs.1 Nr.1 BetrVG vor Ort beim Auftragnehmer ohne Behinderung seiner Betriebsratstätigkeit wahrnehmen kann. Die Bestimmungen des § 11 BDSG werden Inhalt des Dienstleistungsvertrags.

Der Datenschutzbeauftragte der Firma XYZ GmbH überprüft regelmäßig die Einhaltung aller Datenschutzvorschriften in Bezug auf die Anwendung der Kassensysteme. Er berichtet zweimal jährlich dem Betriebsrat. Der Datenschutzbeauftragte stellt dem Betriebsrat die nach § 4 g Abs. 2 BDSG zu führenden Übersichten und die erforderliche Datenschutzzulässigkeitsprüfung des Kassensystems XXX und des Auswertungstools YYY zur Verfügung.

§ 15 – Meinungsverschiedenheiten

Ergeben sich bei der Anwendung und Auslegung dieser Betriebsvereinbarung Meinungsverschiedenheiten bzw. Auslegungsstreitigkeiten, so kann bei Nichteinigung die Einigungsstelle gemäß § 76 BetrVG angerufen werden.

§ 16 – Schlussbestimmungen

Diese Betriebsvereinbarung tritt am Tage ihrer Unterzeichnung in Kraft.

Diese Regelung kann mit einer Frist von vier Monaten von beiden Seiten frühestens zum __.__.___ gekündigt werden. Einvernehmliche Änderungen sind jederzeit möglich.

Bis zum Abschluss einer neuen Regelung bleiben alle Bestimmungen dieser Betriebsvereinbarung in Kraft.

Sollte eine Bestimmung dieser Betriebsvereinbarung unwirksam sein oder werden, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Betriebsparteien verpflichten sich für einen solchen Fall, eine wirksame Regelung zu treffen, die dem Zweck der unwirksamen Regelung möglichst nahe kommt.