15 Fragen zum neuen Datenschutz

BETRIEBSVEREINBARUNGEN *EDV-Betriebsvereinbarungen müssen künftig höheren Ansprüchen genügen. Die wichtigsten 15 Fragen und worauf Betriebsräte achten müssen, klären wir hier.*

VON **WOLFGANG STEEN, MICHAEL FLEISCHMANN** UND **FRANK LORENZ**

Europa hat sich einen eigenen Datenschutz geschaffen. Die umständlich als EU-DSGVO bezeichnete Datenschutzgrundverordnung (nachfolgend: VO) gilt europaweit ab 25. Mai 2018. Der deutsche Gesetzgeber hat am 27. April 2017 ein Anpassungsgesetz verabschiedet, das weiterhin Kollektivvereinbarungen (Betriebsvereinbarungen) zulässt und den bisherigen Beschäftigtendatenschutz (§ 32 BDSG a.F) künftig im neuen, deutlich erweiterten § 26 BDSG-neu regelt. Ob das neue BDSG den Anforderungen der europäischen Vorgaben entspricht, ist umstritten. Im Zweifel müssen gerade Betriebsvereinbarungen den Anforderungen des Artikel 88 Abs. 2 der EU-DSGVO entsprechen, also vor allem den Grundrechtsschutz auch bei Überwachungssystemen am Arbeitsplatz gewährleisten.

1. Müssen bestehende Betriebsvereinbarungen überarbeitet werden?

Ja. Eine »Übergangsregelung« für Alt-Vereinbarungen gibt es nicht. Ab Mai 2018 müssen alle Betriebsvereinbarungen den Anforderungen der VO, insbesondere deren Art. 88 Abs. 2, und des neuen BDSG entsprechen. Zu beachten ist dabei – weiterhin –, dass durch Betriebsvereinbarungen überhaupt erst die gesetzlich geforderte »Erlaubnis« zur Verarbeitung personenbezogener Daten geschaffen wird. Deshalb sind Betriebsvereinbarungen das Steuerungsmittel für den betrieblichen Datenschutz. Dies wird im § 26 Abs. 4 BDSG-neu, gleichzeitig unter Hinweis auf Art. 88 Abs. 2 der VO ausdrücklich hervorgehoben. Nicht ausreichen wird in Zukunft eine pauschale Regelung, nach der dem Arbeitgeber vorbehalten bleibt, »personenbezogene Daten auch auf der Grundlage sonstiger Betriebsvereinbarungen oder einschlägiger gesetzlicher Regelungen zu verarbeiten«. Dagegen steht die Notwendigkeit, jeweils ›angemessene und besondere‹ Maßnahmen zum Persönlichkeitsschutz im Einzelfall regeln zu müssen.

2. Welche wesentlichen Änderungen müssen beachtet werden?

Neben der Neuregelung zur Einwilligung der Erhebung persönlicher Daten (mit Widerrufsrecht) werden für die Praxis relevant: Der Zugang des Betriebsrats zu allen Daten, der geforderte Aufbau eines Datenschutz-Managements im Unternehmen, die Datenschutz-Folgeabschätzung und die Regelungen zur Datenverarbeitung im Ausland.

3. Gibt es weiterhin einen betrieblichen Datenschutzbeauftragten?

Ja. Im Vorfeld der europäischen Diskussionen war das deutsche Modell eines betrieblichen Datenschutzbeauftragten in Frage gestellt. In die endgültige VO wurde dieser schließlich aufgenommen und in das neue BDSG als Verpflichtung, soweit »in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten« beschäftigt werden. In Art. 38 Abs. 3 der VO ist ein Schutzmechanismus zur Bewahrung der Unabhängigkeit des betrieblichen Datenschutzbeauftragten aufgenommen. Er darf

DARUM GEHT ES

1. EDV-Betriebsvereinbarungen müssen künftig der Europäischen Datenschutzverordnung entsprechen.

2. In den Unternehmen muss ein umfangreiches Datenschutzmanagement aufgebaut werden.

3. Mit der Datenschutz-Folgeabschätzung wird ein weites, bisher unbekanntes Terrain für die Betriebsratsarbeit eröffnet

DEFINITIONEN

Datenschutz-Management im Unternehmen
Eine Managementmethode, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

Datenschutz-Folgeabschätzung
Die Datenschutz-Folgeabschätzung ist die Bewertung von Risiken und deren mögliche Folgen für die persönlichen Rechte und Freiheiten der Betroffenen. Sie ist immer dann vorzunehmen, wenn besonders sensible Daten verarbeitet werden oder die Datenverarbeitung dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens, zu bewerten.

keine Anweisungen bei seinen Aufgaben bekommen und darf nicht wegen der Erfüllung dieser Aufgaben abberufen oder benachteiligt werden. Seine Überwachungsfunktion bezieht sich auf Strategien des Unternehmens, die Einhaltung der Datenschutzvorschriften und die Durchführung der Datenschutz-Folgenabschätzung. Unabhängig davon bleibt natürlich der Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG weiterhin verpflichtet und gefordert, die Einhaltung der Datenschutzvorschriften im Betrieb und im Unternehmen zu gewährleisten.

4. Welchen Zugang hat der Betriebsrat zu erhobenen Daten?

Für den Betriebsrat ist in § 26 Abs. 1 BDSG-neu jetzt ausdrücklich ein »Recht auf Daten« bestätigt worden. Es ist den Arbeitgebern danach erlaubt, personenbezogene Daten von Beschäftigten an Betriebsräte dort weiterzugegeben, wo dies gesetzlich (nach § 80 Abs. 2 BetrVG) vorgesehen ist. Der teils noch anzutreffende Versuch, Informationsansprüche des Betriebsrats und anderer Betriebsverfassungsorgane (KBR, GBR, Wirtschaftsausschuss) mit dem Argument »Datenschutz« zu blockieren, dürfte damit endgültig als untauglich anzusehen sein. Der Anspruch auf Daten besteht immer dann, wenn die Daten zur Ausübung der Beteiligungsrechte erforderlich sind, so bei Daten der Verhaltens- und Leistungskontrolle nach § 87 Abs. 1 Nr. 6 BetrVG, bei sozialplanrelevanten Daten oder bei Lohn- und Gehaltsdaten auf Grund der Mitbestimmung nach § 87 Abs. 1 Nr. 10 BetrVG.

5. Welche Daten sind erforderlich im Beschäftigungsverhältnis?

Die Grundaussage im BDSG bleibt, dass die Daten erhoben werden können, die für die Begründung und Durchführung des Beschäftigungsverhältnisses erforderlich sind (§ 26 Abs. 1 BDSG-neu). Allerdings ist eine Verarbeitung der Daten nur zulässig, wenn diese geeignet sowie das mildeste aller gleich effektiven Mittel ist und nicht die schutzwürdigen Interesse des Beschäftigten überwiegen. Das heißt, dass eine verdeckte Videoüberwachung dann zulässig sein kann, wenn der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht und weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind. Allerdings muss sich dann der Verdacht auf einen räumlich und funktional abgrenzbaren Kreis von Arbeitnehmern richten und darf sich nicht auf allgemeine Mutmaßungen beschränken. Nach der Neufassung des § 26 Abs. 1 BDSG müssen nun auch tatsächliche Anhaltspunkte, die den Verdacht begründen dokumentiert werden. Ob also noch anlasslose Taschenkontrollen möglich bleiben, ist zu bezweifeln.

6. Brauchen wir immer die Einwilligung der Betroffenen zur Datenerhebung?

Es ist weiterhin vorgesehen, dass durch Kollektiv-, also Betriebsvereinbarungen, die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten (Gesundheitsdaten) für Zwecke des Beschäftigungsverhältnisses zulässig ist. In § 26 Abs. 4 BDSG-neu wird aber auf die Pflicht der Verhandlungspartner aus Artikel 88 Abs. 2 der VO hingewiesen. Deshalb muss gerade bei Überwachungssystemen (GPS, Telefonüberwachung etc.) darauf geachtet werden, den grundrechtlichen Schutz aus Art. 3 Grundgesetz (Persönlichkeitsrecht und Recht auf informationelle Selbstbestimmung) zu wahren. So wird eine Telefonüberwachung (Recht auf das gesprochene Wort), wenn überhaupt, ohne persönliche Einwilligung der Betroffenen nicht mehr möglich sein. Vorsicht ist geboten bei den besonderen Kategorien personenbezogener Daten. Diese können zwar – mit ausdrücklicher Einwilligung – für Zwecke der Arbeitsmedizin sowie für die Beurteilung der Arbeitsfähigkeit des Beschäftigten erhoben werden, eine Verarbeitung darf hingegen nur von Fachpersonal erfolgen, das zur Verschwiegenheit verpflichtet ist. Wichtig ist, dass eine einmal erteilte Einwilligung jederzeit widerrufen werden kann; ein Widerrufsrecht, über das der Arbeitgeber aufklären muss.

7. Was heißt freiwillige Einwilligung?

Ist eine Einwilligung der Betroffenen in die Datenerhebung und -verarbeitung erforderlich, muss diese künftig »die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist« berücksichtigen (§ 26 Abs. 2 BDSG-neu). Gefordert ist nach der VO vor allem eine Einwilligung ohne Zwang, die also nicht an den Abschluss

eine Arbeitsvertrages geknüpft werden darf (Koppelungsverbot in Art. 7 Abs. 4 VO). Worin eingewilligt werden soll, muss »in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache« vorgelegt werden. Freiwilligkeit wird angenommen, »wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen«. Hier wird es in der Praxis vor allem Diskussionen darüber geben, wessen Interessen beispielsweise bei der GPS-Überwachung überwiegen. In jedem Fall bedarf die Einwilligung nach deutschem Recht der Schriftform.

8. Gibt es neue Informationspflichten des Arbeitgebers?

Ja, und diese sollten auch in der Betriebsvereinbarung festgehalten werden. Die VO fordert in Art. 12, die von einer Datenverarbeitung betroffenen Arbeitnehmer »in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache« über die die gespeicherten Daten sowie Kontaktdaten der verantwortlichen Stelle und des Datenschutzbeauftragten, die Zwecke der Datenverarbeitung, Empfänger der Daten, die Übermittlung der Daten in ein Drittland und die Speicherdauer zu informieren sowie auf die Betroffenenrechte der VO hinzuweisen. Diese Informationspflichten hat auch § 26 Abs. 2 Satz 4 BDSG-neu aufgenommen und den Arbeitgeber zusätzlich verpflichtet, die beschäftigte Person über ihr Widerrufsrecht in Textform aufzuklären.

9. Leistungskontrolle oder »Pseudonymisierung«?

Werden Leistungsdaten von Arbeitnehmern erfasst, stellt sich stets die Frage, ob diese nicht anonymisiert oder pseudonymisiert erfasst werden müssen. Pseudonymisierung bedeutet, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden können. Hier kann schon das Nutzungsverhalten an einer CNC-Maschine zur Notwendigkeit einer Anonymisierung führen, da sonst bereits die Verknüpfung mit dem frei zugänglichen Schichtplan erkennen lässt, wer an der Maschine stand.

Im Übrigen enthält die VO in Art. 22 ein ausdrückliches »Profiling-Verbot«, also ein Verbot der Verarbeitung personenbezogener Daten zum Zweck der Analyse oder Prognose in Bezug auf die Arbeitsleistung – außer diese Verarbeitung ist zwingende Voraussetzung zur Arbeitsvertragserfüllung. Hier werden gänzlich neue Betriebsvereinbarungen erforderlich, um den Persönlichkeitsschutz zu gewährleisten.

10. Was bedeutet Datenschutz-Management?

In Zukunft ist ein betriebliches Management erforderlich, das die Aspekte des Datenschutzes sichert. Hierzu gehören vor allem

- eine die Verarbeitung legitimierende Einwilligung
- ein Verzeichnis von Verarbeitungstätigkeiten
- eine Datenschutz-Folgenabschätzung (Privacy Impact Assessment) und deren Ergebnisse
- die Dokumentation von Datenschutzverletzungen und ergriffene Abwehrmaßnahmen sowie
- umfangreiche Dokumentationspflichten zur Erfüllung der Transparenzpflichten gegenüber Betroffenen

In dieses Management muss der betriebliche Datenschutzbeauftragte eingebunden werden und für den Betriebsrat muss ein fortlaufendes Informationssystem bei Änderungen/Ergänzungen etabliert werden.

11. Was ist unter »technischem Datenschutz« zu verstehen?

Das Schlagwort lautet hier: Technischer vor organisatorischem Datenschutz. Konkret heißt es in Art. 32 VO zum Thema Datensicherheit: »Unter Berücksichtigung des Stands der Technik, ... der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen,

DEFINITION

Regelungen zur Datenverarbeitung im Ausland
Es ergeben sich datenschutzrechtliche Besonderheiten, wenn personenbezogene Daten ins Ausland weitergeleitet bzw. dort verarbeitet werden. Praxisrelevanz gewinnt diese Thematik vor allem in den Bereichen der Auftragsdatenverarbeitung und bei international tätigen Unternehmen. Mehr dazu unter **www.datenschutzbeauftragter-info.de/internationaler-datenschutz**

TERMINHINWEIS

»Das neue Datenschutzgesetz – Anforderungen an ein Datenschutz-Management«
Do. + Fr., 7. + 8.12. 2017
im Hotel Adina am Michel, Hamburg.
Info und Anmeldung: info@brpraxis seminare.de – Tel.: 040 226926-84

um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.« Der Fokus liegt auf dem »Stand der Technik« und dem jeweiligen Schutzbedarf der unterschiedlichen personenbezogenen Daten. Erforderlich wird eine Risikoinventur, in der alle möglichen Bedrohungen und Schwachstellen mit ihrer jeweiligen Eintrittswahrscheinlichkeit und der potenziellen Schwere des Schadens für die Rechte und Freiheiten natürlicher Personen identifiziert werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dafür den BSI-Standard 100–2 vorgelegt, der konkrete Schutzbedarfskategorien enthält. Maßgeblich wird dies vor allem bei steigender Vernetzung von Geräten oder bei Home-Office-Lösungen.

12. Wann wird eine Datenschutz-Folgeabschätzung nötig?

Neu in der VO ist die Pflicht zur Datenschutz-Folgeabschätzung für neu installierte Systeme und Programme. Mindestinhalte sind (a) eine systematische Beschreibung der Prozesse und deren Zwecke inklusive der verfolgten Interessen, (b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit, (c) eine Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen sowie (d) geplante Maßnahmen zur Risikominimierung. Eine Folgeabschätzung ist für alle Auswirkungen der Datenverarbeitung mit neuen Verfahren und Technologien erforderlich, einschließlich der Methoden zur Begrenzung negativer Folgen für die informationelle Selbstbestimmung der betroffenen Personen. Hier dürften vor allem Methoden und Werkzeuge rund um das Thema Arbeit 4.0 eine große Rolle spielen, wenn Risiken einer permanenten Leistungskontrolle vorliegen.

13. Was ändert sich bei einer Datenverarbeitung im Ausland?

Eigentlich kaum etwas. Weiterhin können Daten beispielsweise innerhalb einer Unternehmensgruppe für interne Zwecke (Lohn- und Gehalts- oder Reisekostenabrechnungen etc.) – also mit ausdrücklicher Zweckbindung – nur übermittelt werden, wenn Auftraggeber und Auftragnehmer festgelegte Pflichten einhalten. Dabei wird der Aufragnehmer weitaus mehr in die Pflicht genommen als bisher. Es gilt außerdem das Marktortprinzip, nach dem die EU-Datenschutzregelungen auch auf außerhalb der EU tätige »Verantwortliche« anzuwenden sind, wenn Daten von EU-Bürgern verarbeitet werden. Weiterhin sollten außerhalb der EU ansässige Datenverarbeiter über Binding Corporate Rules (Art. 44 VO) – also verbindliche Richtlinien zum Umgang mit personenbezogenen Daten – oder Standardvertragsklauseln an ein angemessenes Datenschutzniveau gebunden und solche Pflichten in Betriebsvereinbarungen festgelegt werden.

14. Unterliegt auch eine nicht automatisierte Verarbeitung dem Datenschutz?

Ja. Nach dem deutschen BDSG ist auch weiterhin die nicht automatisierte Speicherung oder Verarbeitung von Daten dem Datenschutzgesetz unterworfen. Der Datenschutz ist also auch bei handschriftlichen Aufzeichnungen, bei Einstellungsuntersuchungen, in einem Mitarbeitergespräch oder bei Beobachtungsstudien (Strichlisten) zu gewährleisten. Hier sind meist auch Betriebsvereinbarungen nach § 94 BetrVG erzwingbar (Personalfragebogen).

15. Und was meint das Recht auf Vergessenwerden?

Auch wenn das Recht auf Datensparsamkeit nicht mehr ausdrücklich erwähnt wird, enthält die VO jetzt den Grundsatz der »Datenminimierung« (Art. 5 Abs. 1c) VO) sowie das Recht auf Richtigkeit, so dass personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden müssen. Auch müssen Daten, die nicht mehr (etwa aus steuerlichen Gründen) gebraucht werden, gelöscht werden. Ein solches Vergessenwerden wird sich ebenso auf lange zurück liegende Abmahnungen beziehen müssen ◁

Wolfgang Steen, Fachanwalt für Arbeitsrecht, Gaidies Heggemann & Partner, Hamburg.
www.gsp.de

Michael Fleischmann,
Rechtsanwalt,
sfm-arbeitsrecht, München.
www.sfm-arbeitsrecht.de

Dr. Frank Lorenz,
Rechtsanwalt,
slt-arbeitsrecht, Düsseldorf.
www.slt-arbeitsrecht.de