Stellungnahme

BMI & BMAS Eckpunktepapier Beschäftigtendatenschutz
Mai 2023

Zusammenfassung und übergeordnete Punkte zum Beschäftigtendatenschutz

Adél Holdampf-Wendel
Bereichsleiterin Future of Work & Arbeitsrecht

T +49 30 27576-202
a.holdampf@bitkom.org

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit

T +49 30 27576-161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Im April veröffentlichten BMI und BMAS Vorschläge für eine Novellierung des Beschäftigtendatenschutzes. Bitkom bedankt sich für die Möglichkeit, zu den Eckpunkten Stellung zu nehmen und Vorschläge für den zukünftigen Referentenentwurf zu unterbreiten.

Die Entwicklung von Kriterien und Leitlinien im Bereich des Beschäftigtendatenschutzes ist sicherlich sehr hilfreich. Diese können jedoch nicht erschöpfend sein und sollten nur als Orientierungshilfe dienen, um die Möglichkeit zu erhalten, die Beziehungen zwischen Arbeitgeber und Arbeitnehmer, unter Berücksichtigung der Datenschutzgrundsätze, flexibel zu gestalten.

Bitkom hält die vorgeschlagenen Regelungsfelder für nachvollziehbar und lohnend, auch wenn eine hinreichende und finale Bewertung der Regierungspläne für einen modernen Beschäftigtendatenschutz nur anhand eines konkreten Gesetzentwurfs möglich ist.

Im Folgenden hat Bitkom unter Mitwirkung der Arbeitskreise Datenschutz, Personal- und Arbeitsrecht sowie Arbeit 4.0 Vorschläge für die Schaffung eines Beschäftigtendatenschutzes erarbeitet und nimmt zu den einzelnen Kapiteln des Eckpunktepapiers Stellung. Im ersten Teil werden diejenigen Punkte adressiert, die bisher im Eckpunktepapier noch nicht ausreichend abgedeckt, aber essenziell für ein zukünftiges Beschäftigtendatenschutzrecht sind. Im zweiten Teil werden die einzelnen Aspekte des Eckpunktepapiers bewertet.

Zielstellung und Notwendigkeit neuer Regelungen

Die DS-GVO will eine definitive Harmonisierung des Datenschutzrechts in der EU sicherstellen. Ihr gegenüber steht ein fragmentiertes, nur in Teilen harmonisiertes

Arbeitsrecht in der EU. Zaghafte Versuche zu einer Harmonisierung wenigstens der Datenschutzregelungen scheiterten am Widerstand mehrerer Mitgliedstaaten. Dabei sind einheitliche europäische HR-Prozesse für alle Marktteilnehmer äußerst wichtig. Das gilt nicht nur für international agierende Unternehmen. Für kleine und mittelständische Unternehmen machen einheitliche Prozesse die Vorteile des Binnenmarkts besonders greifbar.

Viele Personaldienstleistungen werden nicht nur in Deutschland erbracht, sondern in mehreren Gesellschaften in verschiedenen Mitgliedstaaten oder im Konzern gebündelt von einer Gesellschaft für mehrere andere Gesellschaften. Es wird arbeitsteilig verfahren und die Zeiten, in denen alle Gesellschaften einer Gruppe ganz eigenständig agierten sind – falls es sie jemals gab – schon Jahrzehnte vor der DS-GVO vergangen. Deshalb ist es wichtig, dass nationale Regelungen im Beschäftigtendatenschutz immer die europäische Perspektive und den Harmonisierungsgedanken der DS-GVO im Blick haben. Sonderwege verbieten sich und Regelungen, die gut gemeint sind, sich aber alsbald als unionsrechtswidrig herausstellen, ebenso.

Technologienutzung und Technologieneutralität

Der technologieneutrale Ansatz der Vorschläge ist grundsätzlich zu begrüßen. Bis auf den Bereich KI ist aber von innovativen technischen Entwicklungen, die sich disruptiv auf den Bereich HR auswirken, bedauerlicherweise wenig enthalten. Hier müsste z.B. auch der Bereich des Metaverse und seiner Auswirkungen für das Arbeiten von Morgen adressiert werden. Leider dient hier wohl der technologieneutrale Ansatz als Ausrede für bisher fehlendes Engagement solche Themen anzugehen. Das eine schließt jedoch das andere nicht aus und sollte ausdrücklich adressiert werden.

Konzernverbünde

Wir begrüßen insbesondere den Vorschlag, welcher Datenübermittlungen zwischen konzernverbundenen Unternehmen vereinfachen und rechtssicherer gestalten will. Die Arbeit in agilen und Matrix Strukturen über verschiedene Konzernunternehmen hinweg gewinnt immer mehr an Bedeutung und sogenannte „shared services“ nehmen zentrale Aufgaben für mehrere Gesellschaften im Konzern wahr. Die Umsetzung der datenschutzrechtlichen Regelungen bindet hier aktuell erhebliche Ressourcen für komplexe und umfassende Regelungen über Auftragsdatenverarbeitungsverträge, Joint Controller Regelungen und Dienstleistungen im berechtigten Interesse.

Eine Vereinfachung konzerninterner Datenübermittlung kann den administrativen Aufwand erheblich reduzieren und zur Rechtssicherheit beitragen.

Überarbeitung von § 26 BDSG

Im Hinblick auf die Entscheidung des EuGH vom 30.03.2023 (C-34/21) zu § 26 des Hessischen Datenschutzgesetzes und der schon jetzt absehbaren Konsequenz für § 26 BDSG ist es notwendig, den bisherigen § 26 BDSG nachzubessern. Er ist unzweckmäßig und unionsrechtswidrig. Denn er wiederholt in weiten Teilen Art. 6 DS-GVO, was bei Verordnungen unzulässig ist.

Stattdessen sollte bei der Neufassung des § 26 BDSG klargestellt werden, dass Kollektivvereinbarungen ebenfalls die Verarbeitung von personenbezogenen Daten rechtfertigen können. Dies wäre von der Ermächtigung des Art. 88 DS-GVO gedeckt. Regelungen, die nur die DS-GVO umformulieren und wiederholen, sind zu vermeiden.

Bei der Neufassung des Bundesdatenschutzgesetzes sollte darauf geachtet werden, dass die weiteren bestehenden Fehler beseitigt werden. § 24 Abs. 2 BDSG enthält einen solchen Fehler, der ihn unionsrechtswidrig macht, denn er wiederholt im wesentlichen Art. 9 Abs. 1 und 2 DS-GVO. Das ist weder zweckmäßig noch zulässig. Vielmehr ist die Verarbeitung von Gesundheitsdaten durch den Arbeitgeber bereits durch Art. 6 Abs. 1 lit. b i.V.m. Art. 9 Abs. 2 lit. b, c, g, h DS-GVO in Verbindung mit den bestehenden Vorschriften (beispielsweise für das betriebliche Eingliederungsmanagement gem. § 167 Abs. 2 SBG IX) gerechtfertigt. Der Gesetzgeber darf nicht erneut den Fehler machen, bestehende Regelungen zu wiederholen.

Die Regelungen zur Einwilligung sind ebenfalls überflüssig. Insbesondere Art. 6 Abs. 1 lit. a und Art. 7 Abs. 4 DS-GVO schützen die Beschäftigten bereits umfassend.

Betriebsverfassungsrechtliche Regelungen

Eine zeitgemäße Änderung der betriebsverfassungsrechtlichen Regelungen ist ebenfalls unzureichend adressiert. Es bedarf einer Anpassung der Mitbestimmung, insbesondere hinsichtlich §§ 87 Abs. 1 Nr. 6 und 80 Abs. 2 BetrVG.

Zudem muss die Kohärenz der neuen Regeln für den Beschäftigtendatenschutz mit der geplanten Novelle des Betriebsverfassungsgesetzes sichergestellt werden.

Neben der Anpassung des § 80 Abs. 2 BetrVG (s. Anmerkungen zum Punkt „Mitbestimmung weiterentwickeln – Beschäftigtendatenschutz stärken“) wäre eine praxistaugliche Anpassung des § 87 Abs. Abs. 1 Nr. 6 BetrVG wünschenswert. Sinn und Zweck des Mitbestimmungsrechts bei Maßnahmen zur Überwachung des Verhaltens oder Leistung der Arbeitnehmer im Sinne von § 87 Abs. 1 Nr. 6 BetrVG ist, dass solche Überwachungsmaßnahmen ins allgemeine Persönlichkeitsrecht des Arbeitnehmers eingreifen und der Arbeitnehmer davor geschützt werden soll. Es ist daher sinnvoll, wenn solche Maßnahmen dem Mitbestimmungsrecht des Betriebsrats unterliegen. Allerdings muss hierbei auch die Praxisauswirkung beachtet werden: Die Rechtswirklichkeit und damit das Mitbestimmungsrecht gehen deutlich weiter als nur bei echten Überwachungsmaßnahmen. § 87 Abs. 1 Nr. 6 BetrVG umfasst rein vom Wortlaut zwar nur die „Einführung und Anwendung von technischen Einrichtungen,

die dazu *bestimmt* sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Die ständige BAG-Rechtsprechung ist jedoch eine andere und seit 1975 (!) unverändert. Sie versteht Nr. 6 dahingehend, dass der Tatbestand bei jeder technischen Anwendung bereits erfüllt ist, wenn die technische Einrichtung objektiv *geeignet* ist, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen. Diese Rechtsprechung stammt damit aus einer Zeit, als eine IT-Infrastruktur wie die heutige nicht mal in Ansätzen existierte, geschweige denn vorstellbar war.

Die Vorschrift des § 87 Abs. 1 Nr. 6 BetrVG hat durch die weite Auslegung der Rechtsprechung gepaart mit der rasanten Entwicklung der Informationstechnologie eine ungeahnte Bedeutung erlangt. Jegliche IT-Produkte, auch Standardprodukte wie z.B. MS-Office, die unserer Arbeitserleichterung und der Kollaboration dienen, fallen unter § 87 Abs. 1 Nr. 6 BetrVG, weil sie nach BAG-Rechtsprechung objektiv zur Überwachung geeignet sind, weil z.B. Nutzungsprotokolle vom Arbeitgeber ausgelesen werden könnten. Allein das Potential zur Überwachung genügt, sodass ein Mitbestimmungsrecht greift, ohne dass von einer Persönlichkeitsrechtsverletzung hier die Rede sein kann. Dies geht deutlich zu weit und die Praxisauswirkungen sind massiv. IT-Produkte gehören heute zum Arbeitsleben wie die Büroausstattung. Deswegen muss sich auf den ursprünglichen Sinn und Zweck von § 87 Abs. 1 Nr. 6 BetrVG besonnen werden. Eine entsprechende engere Formulierung im Gesetz und damit praktikable Lösung ist essenziell. Diese Regelung muss die Mitbestimmung des Betriebsrats auf die tatsächliche Nutzung von Daten zur Überwachung des Verhaltens oder Leistung der Arbeitnehmer beschränken.

Zumindest müssen aber aus dem Anwendungsbereich des § 87 Abs. 1 Nr. 6 BetrVG alle Fälle ausgenommen werden, bei denen personenbezogene Daten zur Sicherung von IT-Systemen in dem Umfang verarbeitet werden, den Art. 32 Abs. 1, vor allem lit. b und c DS-GVO verlangen. Denn diese Daten könnten zur Verhaltens- und Leistungskontrolle eingesetzt werden, werden aber im Rahmen des Art. 32 Abs. 1 DS-GVO dazu gerade nicht verarbeitet. Die ausufernde Rechtsprechung des BAG führt in der Praxis dazu, dass kein DS-GVO-konformes IT-System (ein solches benötigt eine personenbezogene Zugangs- und Zugriffs- sowie Verlaufskontrolle) eingesetzt werden kann, ohne dass hierzu eine Betriebsvereinbarung geschlossen wird.

Unter den vorgenannten Aspekten bleibt das Konzeptpapier bisher deutlich hinter den Möglichkeiten zurück, praktischen Notwendigkeiten und betriebliche Wirklichkeit zu adressieren und wichtige Rechtsfragen zu klären.

Privatnutzung dienstlicher Telekommunikationsdienste

Es fehlt weiterhin ein Vorschlag zum Umgang des Arbeitgebers mit dienstlichen Telekommunikationsdiensten bei erlaubter bzw. geduldeter Privatnutzung von Beschäftigten. Hier braucht es die Klarstellung, dass Arbeitgeber bei erlaubter oder geduldeter Privatnutzung dienstlicher Telekommunikationsdienste keine Diensteanbieter sind und damit für sie das Fernmeldegeheimnis in § 3 TTDSG nicht gilt.

Derzeit wird ein Arbeitgeber zum Diensteanbieter im Sinne des § 3 TTDSG, falls er seinen Beschäftigten die private Nutzung dienstlich bereit gestellter Telekommunikationsdienste gestattet oder diese Nutzung duldet. Er muss sich so behandeln lassen, als verdiene er mit dieser erlaubten Privatnutzung Geld. Dieses Ergebnis ist absurd. Es bestraft den Arbeitgeber für einen großzügigen Umgang mit seinen Ressourcen. Die jetzige Fehllage hat zur Folge, dass der Arbeitgeber vor allem das Fernmeldegeheimnis gegenüber den Beschäftigten beachten muss. Notwendige Auswertungen können nicht vorgenommen werden und der Arbeitgeber setzt sich dem Risiko aus, eine Straftat nach § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) zu begehen, wenn er seine Telekommunikationsinfrastruktur sichert. Völlig aus dem Blick gerät, dass er keineswegs gewerbliche Telekommunikationsdienste erbringt – nicht für seine Beschäftigten, und erst recht nicht für Dritte, die mit diesen in privaten Kontakt treten. Er darf auch nicht als Anbieter von Telekommunikationsdiensten im Sinne von § 3 Nr. 1 TKG gelten. Da die Rechtsprechung dies überwiegend aufgrund der geltenden Rechtslage falsch sieht, ist eine gesetzliche neue Regelung unumgänglich.

Deshalb sollte klargestellt werden, dass Arbeitgeber bei erlaubter oder geduldeter Privatnutzung dienstlicher Telekommunikationsdienste keine Diensteanbieter sind und damit das Fernmeldegeheimnis aus § 3 TTDSG nicht gilt. Dies wäre nicht nur zum Vorteil des Arbeitgebers, sondern auch der Beschäftigten, weil die Arbeitgeber die (zeitlich begrenzte) Privatnutzung bedenkenlos erlauben könnten und sich die Beschäftigten nicht mehr in einer Grauzone bewegen müssten.

Anmerkungen zum Eckpunktepapier

Weiter Anwendungsbereich

Die Erläuterungen zum sachlichen Anwendungsbereich scheinen verfehlt und bergen die Gefahr der Europarechtswidrigkeit. Denn der EuGH hat in seiner Entscheidung vom 30.03.3023 (C-34/21) klar die Begriffe "Beschäftigter" und "Beschäftigungskontext" i.S.d. DS-GVO definiert (Rn. 42 und 43) und dabei festgestellt, dass das sowohl für private als auch öffentliche Arbeitgeber gilt. Der deutsche Gesetzgeber tut also gut daran, sich an dieser Definition zu orientieren, will man nicht Gefahr laufen, dass der EuGH das neue Gesetz sogleich wieder kassiert. Die angedachte explizite Inklusion von Crowdworkern ist entgegen anderer bisher vertretener Ansicht von Teilen des Schrifttums zwar grundsätzlich möglich, aber unnötig. Denn die vom EuGH in vorgenannter Entscheidung sehr weit definierten Begriffe "Beschäftigter" und "Beschäftigungskontext" im datenschutzrechtlichen Kontext umfassen bereits solo-selbständige Plattformtätige.

Eine spezifische Ausdehnung der datenschutzrechtlichen Regelungen auf solo-selbstständige Plattformtätige erscheint auch aufgrund der Rechtsprechung des BAG

zu Plattformbeschäftigten und deren Einordnung als Arbeitnehmer bei Vorliegen bestimmter Voraussetzungen nicht erforderlich. Eine pauschale Einbeziehung von allen Plattformtätigen würde jedoch die mögliche Einordnung von Plattformtätigen als Selbstständige vernachlässigen.

In diesem Zusammenhang sind auch die Regelungen des EU-Richtlinienentwurfs zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit zu beachten. Im Zentrum des Regelungsvorhabens steht die richtige Einordnung des Beschäftigungsstatus von Plattformtätigen als Arbeitnehmer oder Selbstständige. Der Richtlinienentwurf enthält aber auch Transparenzvorschriften und Regelungen zum Schutz der personenbezogenen Daten von Plattformtätigen beim algorithmischen Management im Kontext der Plattformarbeit. Das EU-Parlament hat in erster Lesung diese speziellen Datenschutzbestimmungen erweitert.

Mögliche Änderungen im weiteren Verlauf des EU-Gesetzgebungsverfahrens sollten daher abgewartet werden, um eine EU-rechtskonforme nationale Gesetzgebung zu erreichen.

Überwachung und Kontrolle begrenzen

Die Vorschläge zur Überwachung und Kontrolle scheinen sich stark an der Rechtsprechung und der bereits bestehenden Rechtslage zu orientieren.

So ist beispielsweise die verdeckte Überwachung zur Aufdeckung von Straftaten durch die Rechtsprechung bereits stark eingeschränkt und orientiert sich jeweils an der Verhältnismäßigkeit der Maßnahme. Danach ist eine verdeckte Videoüberwachung nur als letztes Mittel zur Wahrung des Kontrollinteresses des Arbeitgebers möglich. Dieses Interesse des Arbeitgebers muss auch bei einer möglichen gesetzlichen Regelung (nicht nur in Bezug auf die verdeckte Videoüberwachung, sondern generell) berücksichtigt und mit dem Persönlichkeitsrecht der Arbeitnehmer in Einklang gebracht werden. Die Umsetzung in Gesetzesform dürfte sich schwierig gestalten, da es sich häufig um eine Frage der Abwägung, gerade im Zusammenhang mit Erforderlichkeit, handelt. Wegen der damit verbundenen Transparenz wäre eine Regelung gleichwohl zu begrüßen.

Wichtig ist dabei jedoch, Unterscheidungen der Anwendungen hinsichtlich Einsatzzweck und konkreter Funktionsweisen weiterhin zu ermöglichen und keine Pauschalverbote einzuziehen. Es bedarf einer Unterscheidung zwischen Datenerhebung und Anwendungsfällen. Nur konkrete, klar abgrenzbare Anwendungsfälle sollten reguliert werden. Aus praktischer Perspektive und im Interesse der Kundinnen und Kunden besteht ein großes Interesse, so viele Prozesse wie möglich zu analysieren, um den Service und die Leistungen zu optimieren und Sicherheitsvorgaben umzusetzen. Unternehmen müssen in der Lage sein, produkt- oder arbeitsablaufbezogene Daten (auch dauerhaft) zu erfassen, um Arbeitsabläufe verfolgen und nachvollziehen zu können, auch wenn die Daten dauerhaft und individuell erhoben werden. Es besteht keine automatische Verknüpfung zwischen dauerhafter Datenerhebung und Überwachungsdruck bzw. illegaler Überwachung. Die

legitimen Zwecke der Datenerhebung sollten sich nicht ausschließlich auf Sicherheitsaspekte beschränken, sondern auch begründete Geschäftszwecke umfassen. Neue Regulierung muss die Persönlichkeitsrechte und technische Innovationen zusammenbringen, denn KI und Maschinelles Lernen gewinnen immer mehr an Bedeutung für ein effektives und effizientes Personalmanagement.

Darüber hinaus ist zu beachten, dass im Gegensatz zum geltenden § 26 Abs. 1 S. 2 BDSG und der im Positionspapier genannten Einschränkung Verarbeitungen nicht nur zur Aufdeckung des Verdachts von im Beschäftigungsverhältnis begangenen Straftaten, sondern auch von schwerwiegenden arbeitsvertraglichen Pflichtverletzungen und Ordnungswidrigkeiten erfasst sein sollen. Diese Erweiterung ist folgerichtig und stellt eine sinnvolle Ergänzung dar.

Einsatz Künstlicher Intelligenz: Transparenz schafft Vertrauen

Hier ist zunächst die Entwicklung der europäischen Gesetzgebung zur KI-Verordnung abzuwarten. Es mag richtig sein, die Black-Box-Problematik aufzugreifen und dafür zu sorgen, dass KI erklärbar bleibt, wie es auch von der EU beabsichtigt ist. Allerdings sollten dadurch nicht die Arbeitgeber zu stark belastet werden, um deren Wettbewerbsfähigkeit im internationalen Vergleich zu erhalten.

Mit Regelungen für typische Datenverarbeitungsvorgänge im Beschäftigungskontext, die auf KI/Algorithmen basieren (diese können natürlich nicht abschließend sein) sowie der Stärkung von Transparenz würde der deutsche Gesetzgeber zwei der Hauptkritikpunkte aus datenschutzrechtlicher Sicht (die sich auch im aktuellen Verfahren der italienischen Datenschutzbehörde gegen den Betreiber von ChatGPT wiederfinden) adressieren. Das ist begrüßenswert. Unerwähnt bleibt aber derzeit noch insbesondere die Frage nach der Löschbarkeit via KI verarbeiteter Daten; ein Thema, welches sich insbesondere bei „Large Language Models (LLM)“ wie ChatGPT stellt. Zu beachten ist allerdings, dass eine zu starke Beschränkung bzw. Regulierung von KI-Anwendungen – die mittlerweile sehr verbreitet im Bereich HR sind – deutsche Arbeitgeber im Vergleich zu europäischen Wettbewerbern benachteiligen würde. Hier sollte sich die Bundesregierung für eine praxistaugliche KI-Regulierung auf EU-Ebene einsetzen, anstatt eine Insellösung zu schaffen, um der Verflechtung einer globalisierten und digitalisierten Welt gerecht zu werden.

Zudem könnte eine Regelung eingeführt werden, die Arbeitgeber unter bestimmten Voraussetzungen verpflichtet, die Funktionsweise der eingesetzten KI zu erläutern (wie dies z.B. auch im EU-Richtlinienentwurf zur Plattformarbeit vorgesehen ist). Dabei sollten die Arbeitgeber jedoch nicht pauschal verpflichtet werden, da die Einsatzmöglichkeiten von künstlicher Intelligenz sehr vielfältig sind und die Erklärungspflichten daher ausufern würden. Vielmehr sollte eine Abwägung erfolgen und strenge Voraussetzungen für das Auslösen einer solchen Pflicht geschaffen werden, z.B. in Abhängigkeit von der Bedeutung der eingesetzten Technik für den Betriebsablauf, des KI-immanenten Risikos und der Erforderlichkeit und Verhältnismäßigkeit (vor allem in Bezug auf Geschäftsgeheimnisse), um so auch die

Haftungsregelungen für KI zu erleichtern, aber auch die Arbeitgeberinteressen entsprechend zu berücksichtigen. Dies würde auch den Willen des EU-Gesetzgebers widerspiegeln.

Zudem ist fraglich, ob die Regelung in Art. 22 DS-GVO nicht bereits für den Einsatz von KI ausreichend ist. Hauptargument für die Entwicklung neuer Regelungen für KI ist es, dass keine „biased" Entscheidungen durch die Algorithmen und deren Datenfütterung getroffen werden. Allerdings sieht Art. 22 DS-GVO eben vor, die endgültige Entscheidung beim Menschen zu belassen, wenn automatisierte Entscheidungen entwickelt werden, die rechtliche Wirkung entfalten. Zudem gibt die Regelung auch den Schutz besonderer personenbezogener Daten vor (Art. 22 Abs. 4 DS-GVO).

Besonderer Schutz im Bewerbungsverfahren

Bei diesem Vorschlag ist zu beachten, dass die Regelungen der DS-GVO und des BDSG bereits auf das Bewerbungsverfahren anwendbar sind und der damit verbundene Schutzstandard besteht. Nach § 26 Abs. 8 Satz 2 BDSG sind auch Bewerberinnen und Bewerber Beschäftigte. Die hier genannten Aspekte sind bereits durch die Rechtsprechung und teilweise durch das AGG definierte Verbote.

Eine entsprechende Regelung nach diesem Vorschlag wäre nur aus Transparenzgründen, nicht aber zur rechtlichen Entwicklung, erforderlich.

Das bisher fast ausschließlich durch Richterrecht etablierte Fragerecht des Arbeitgebers gesetzlich anhand typisierender Regelbeispiele zu normieren ist daher zwar ein ehrenhaftes Anliegen, dürfte aber aufgrund der Fülle der Kasuistik der letzten Jahrzehnte kaum praxisgerecht abbildbar sein. Im Datenschutzrecht wäre es zudem systematisch nicht korrekt verankert.

Der Grundsatz der Direkterhebung (vgl. § 4 Abs. 2 S. 2 BDSG a.F.) ist in der DS-GVO (bewusst) nicht mehr enthalten. Ihm wird in Deutschland aber immer noch seitens Aufsichtsbehörden und Schrifttum sowie nun auch des deutschen Gesetzgebers nachgetrauert. Im Anbahnungsverhältnis zwischen Arbeitgeber und Bewerber hat er aber grundsätzlich seine Berechtigung. Dies folgt bereits aus dem Transparenzgebot des Art. 88 Abs. 2 DS-GVO, welcher durch die jüngste EuGH-Rechtsprechung nochmal an Bedeutung gewonnen hat. Hier braucht es also nicht zwingend einer gesetzlichen Klarstellung, denn unstreitig ergibt sich für deutsche Arbeitgeber bereits nach Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) und der in den §§ 241 Abs. 2, 242 BGB verankerten Rücksichtnahmepflicht des Arbeitgebers bereits das Gebot personenbezogene Daten möglichst beim Bewerber selbst zu erheben. Im Falle einer gesetzlichen Klarstellung sollte hier folglich zumindest die Einschränkung erfolgen, Daten "in der Regel" beim Bewerber zu erheben, und keine pauschale Verpflichtung zur regelmäßigen Direkterhebung. Denn die DS-GVO stellt Direkterhebung und nicht direkte Erhebung beim Betroffenen zumindest formal gleich (vgl. Art. 13 und 14 DS-GVO) und in manchen Situationen – beispielsweise Erkundigungen beim ehemaligen Arbeitgeber – ist eine Direkterhebung beim Betroffenen per se auch gar nicht möglich.

Eine Regelung über medizinische Eignungsuntersuchungen im Bewerbungsverfahren wäre eine sinnvolle Ergänzung der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) und würde eine entsprechende rechtliche unklare Zone schließen.

Rechtssicherheit beim Schutz besonders sensibler Daten

Auch hier handelt es sich um eine potentielle Regelung, die bereits in der DS-GVO und im BDSG geregelt ist. Der Schutz besonders sensibler Daten ist in Art. 9 DS-GVO geregelt. Im § 26 Abs. 3 BDSG findet sich eine Konkretisierung in Bezug auf Beschäftigungsverhältnisse. Dort sind auch bereits zulässige Sachverhalte genannt, in denen die Verarbeitung sensibler Daten möglich ist.

Interessenabwägung handhabbarer machen

Die erwähnten Faktoren sind grundsätzlich geeignet, eine Interessenabwägung in der Praxis zu konkretisieren. Weitere Kriterien könnten bestimmte und nach Risikokriterien zu bewertende Drittlandstransfers, risikominierende Maßnahmen wie Pseudonymisierung oder Verschlüsselung sowie Vorhersehbarkeit für und Transparenz gegenüber Betroffenen sein. Insbesondere hinsichtlich der letzten Punkte tut der Gesetzgeber gut daran, die entsprechende EuGH-Rechtsprechung (z.B. C-275/06, C-597/19) sowie Vorgaben aus ErwG 47 DS-GVO zu beachten. Eine abschließende Regelung von Kriterien zur Interessenabwägung ist im Lichte der EuGH-Rechtsprechung (C-13/16) jedenfalls nicht möglich, da sie grundsätzlich von den konkreten Umständen des betreffenden Einzelfalls abhängt.

Die Festlegung der im Vorschlag genannten Kriterien ist also aus Gründen der Transparenz zu befürworten. Allerdings handelt es sich bei dem Vorschlag auch um die Wiedergabe bereits bestehender Anforderungen. Die Verhältnismäßigkeit der Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses ist unter Beachtung der Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne bereits in § 26 BDSG normiert. Eine Ergänzung der Norm um die Kriterien der Erforderlichkeit erscheint daher zweckmäßiger als die Schaffung eines neuen Gesetzes. Zudem dürfte sich die Festlegung der Kriterien schwierig gestalten, da die Interessenabwägung einzelfallbezogen ist und sich je nach Beschäftigungsphase unterscheidet.

Freiwilligkeit sicherstellen: Klare Regelungen für Einwilligungen

Die Einwilligung ist ein zumindest teilweise in der Praxis genutzter Erlaubnistatbestand, der jedoch mit Rechtsunsicherheiten und auch Praxisproblemen behaftet ist. Sie wird als Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungskontext sehr zurückhaltend verwendet, da sie widerruflich und somit für eine dauerhafte Datenverarbeitung ohnehin nicht verlässlich ist.

Aufgrund der bereits existierenden Beschränkungen der Einwilligung – vor allem für besondere personenbezogene Daten – werden die Interessen der Arbeitnehmer gewahrt. Zwingende arbeitsrechtliche Schutznormen und -prinzipien können auch nicht durch die Einwilligung ausgehebelt werden.

Klare gesetzliche Anforderungen für die Freiwilligkeit einer Einwilligung im Beschäftigungskontext sind für die Praxis hilfreich, denn damit würde einer der typischen Zankäpfel, insbesondere in Auseinandersetzungen mit den Aufsichtsbehörden, entschärft und zu mehr Rechtssicherheit beitragen. Denn bis in die jüngste Zeit haben deutsche Behörden die Möglichkeit der Einwilligung im Beschäftigungskontext pauschal aufgrund fehlender Freiwilligkeit verneint bzw. sodann so hohe Anforderungen an den Freiwilligkeitscharakter gestellt, dass das Institut der Einwilligung in der Praxis faktisch nicht umsetzbar gewesen wäre. Dabei hat bereits zum alten Recht das BAG (8 AZR 1010/13) klargestellt, dass von einer generellen Unwirksamkeit der Einwilligung von Arbeitnehmern, weil diese im Rahmen eines Arbeitsverhältnisses nicht „frei entscheiden“ könnten, nicht auszugehen ist.

Eine weitere gesetzliche Einschränkung der Einwilligung sollte aber nicht stattfinden. Zu beachten ist, dass die Einwilligung der einzige Erlaubnistatbestand, der dem Betroffenen die Entscheidung über die Legitimation der Datenverarbeitung überlässt.

Der Einwilligende entscheidet sich mit seiner Erklärung für die Verarbeitung seiner personenbezogenen Daten. Willigt er hingegen nicht ein, darf eine Verarbeitung nur dann erfolgen, wenn ein anderer Erlaubnistatbestand erfüllt ist.

Somit wird die Einwilligung auch den Interessen des Betroffenen gerecht, da die Rechtmäßigkeit der Datenverarbeitung seiner Kontrolle unterliegt. Konstellationen, in denen die Datenverarbeitung trotz anderer fehlender Erlaubnistatbestände vom Beschäftigten gewünscht wird, sind vielfältig.

Mehr Rechtssicherheit bei der Datenverarbeitung in Konzernen

Der Abbau bürokratischer Hürden und die Vereinfachung der konzerninternen Datenübermittlung trägt den Bedürfnissen der Praxis Rechnung und ist daher zu begrüßen. Die konzerninterne Datenübermittlung ist weit verbreitet, aber bisher weder in der DS-GVO noch im BDSG geregelt. Vielmehr ist die Datenübermittlung nach den Erwägungsgründen zur DS-GVO nur vom Interesse interner Verwaltungszwecke gedeckt. Es bedürfte daher einer eigenen materiell-rechtlichen Grundlage für die Datenübermittlung. Der Abbau bürokratischer Hürden im Bereich der konzerninternen Datenverarbeitung und -übermittlung ist daher zu unterstützen. Es ist eine Regelung erforderlich, die es den Konzernen erlaubt, Daten zu Geschäftszwecken und zur Durchführung von Geschäftstätigkeiten und Verwaltungsprozessen zu übermitteln.

Betroffenenrechte sichern und ergänzen

Die Notwendigkeit einer Neuregelung ist fraglich. Die Betroffenen können - wie auch im Vorschlag erwähnt - ihre Rechte über die DS-GVO geltend machen. Dies gilt auch für den im Vorschlag erwähnten Anspruch auf Löschung von Bewerberdaten, der in Art. 17 DS-GVO normiert ist. Auch weitergehende Ansprüche wie Schadensersatz sind bereits normiert und durch die Rechtsprechung konkretisiert.

Zu den wenigen prozessualen Verwertungsverboten im Arbeitsrecht gibt es Rechtsprechung, die zeigt, dass es sich immer um eine Einzelfallentscheidung handelt. Zentral ist dabei immer die Interessenabwägung zwischen dem Persönlichkeitsrecht des Arbeitnehmers und dem Beweisnotstand des Arbeitgebers. Eine feste Regelung scheint hier kaum möglich.

Die Rechte der Betroffenen sind bereits durch die bestehenden Gesetze und die Rechtsprechung hinreichend gesichert. Ergänzungen sind daher nicht erforderlich.

BYOD: Privates von Dienstlichem trennen

Die Nutzung von privaten Endgeräten des Arbeitnehmers birgt für den Arbeitgeber datenschutzrechtliche Risiken, da keine Kontrolle durch den Arbeitgeber besteht. Daher sind häufig besondere technische Vorkehrungen zur Trennung privater und dienstlicher Daten bzw. zur Verhinderung der Verbreitung vertraulicher Daten erforderlich. Dem kann z. B. durch getrennte Benutzerbereiche entgegengewirkt werden.

Aufgrund der Risiken kann über eine entsprechende gesetzliche Regelung nachgedacht werden. Insbesondere sollte ein Fernzugriff des Arbeitgebers auf den dienstlich genutzten Teil des Gerätes des Arbeitnehmers möglich sein. Im Übrigen können Regelungen hierzu auch in Betriebsvereinbarungen unter Beachtung der bestehenden Datenschutzbestimmungen getroffen werden.

Praktische Realitäten machen es in jedem Fall erforderlich, dass BYOD weiterhin ermöglicht wird und z.B. das Aufspielen betrieblicher Software zur Erbringung der vereinbarten Leistung erlaubt bleibt.

Es müssen zudem die Interessen der IT-Sicherheit berücksichtigt werden. Angreifer können gerade über Beschäftigte in das Unternehmen eindringen und mittels Ransomware ganze Unternehmensgruppen lahmlegen und erpressen. Dies gilt dann auch für die Daten und Arbeitsplätze der Beschäftigten. Dies ist ein Wettlauf der Technik und erfordert einen wirksamen Schutz und die Möglichkeit, jede Verbindung in das und im Unternehmensnetzwerk auf solche Angriffe hin zu kontrollieren.

Mitbestimmung weiterentwickeln – Beschäftigtendatenschutz stärken

Die Einbeziehung der Arbeitnehmer in den Beschäftigtendatenschutz hat bereits im Betriebsverfassungsgesetz (BetrVG) einen hohen Stellenwert. Das Mitbestimmungsrecht des Betriebsrats bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ (§ 87 Abs. 1 Nr. 6 BetrVG) wird bereits sehr weit ausgelegt, so dass der Betriebsrat bereits bei der Einführung der meisten technischen Einrichtungen zu beteiligen ist. In diesem Zusammenhang ist darauf hinzuweisen, dass die Gestaltung des Betriebes mit technischen Mitteln außerhalb dieses Mitbestimmungsrechts als abstrakte planerische Entscheidung des Arbeitgebers einzuordnen ist, die von der unternehmerischen Freiheit gedeckt sein sollte.

Die bisherigen Vorschläge des BMAS und des BMI lesen sich so, als ob dem Betriebs- bzw. dem Personalrat zukünftig Aufgaben übertragen werden sollen, die qua DS-GVO explizit dem Datenschutzbeauftragten (DSB) zufallen und vorbehalten sind. Die Überwachung des Datenschutzes ist aber absolut nicht Aufgabe des Betriebsrats (BR), sondern des DSB und der Aufsichtsbehörden. Insoweit sperren Art. 37-39 DS-GVO auch mögliche zukünftige Regelungen im BetrVG, die solche Aufgaben dem BR übertragen wollten. Der BR hat hier bereits mit §§ 80, 87 BetrVG ein ausreichendes Instrumentarium zur Hand, und muss sich ausweislich § 79a BetrVG bei seiner Tätigkeit selbst an die DS-GVO halten. Die in Teilen der arbeitsrechtlichen Literatur vertretene Ansicht, wonach die gem. Art. 38 Abs. 1 lit. b DS-GVO dem DSB übertragene Aufgabe, die Einhaltung des Datenschutzes sicherzustellen und zu überwachen, berühre nicht die Überwachungsaufgabe des Betriebsrats, sondern sie verdoppele vielmehr die Kontrolle, verfängt nicht. Denn die DS-GVO überträgt diese Aufgabe neben den Aufsichtsbehörden ausschließlich und abschließend der Funktion des DSB. Zwar ließe sich dieser Konflikt auflösen, soweit ein BR-Mitglied zudem auch als DSB benannt ist. Das würde jedoch inzident eine weitere Baustelle schaffen, nämlich das Thema Unabhängigkeit und Interessenskonflikte. Neben dieser dogmatischen Hürde gibt es auch noch eine Praktische: denn eine zweifache Zuständigkeit für den Datenschutz sowohl des DSB als auch BR ist nicht praktikabel. Dies führt nämlich zwangsläufig zu unnötigen Zuständigkeitsdebatten in Unternehmen, lähmt die effektive Umsetzung des Datenschutzes und verkehrt damit das angestrebte Ziel Beschäftigte und deren Rechte sowie berechtigte Interessen zu schützen ins Gegenteil.

Der Datenschutzbeauftragte, der weisungsfrei und gegen Maßregelung besonders geschützt ist, ist die durch die DS-GVO allein berufene Instanz der innerbetrieblichen Datenschutzkontrolle. Auch den Betriebsräten steht der betriebliche Datenschutzbeauftragte als weisungsfreier Experte zur Verfügung.

Im § 80 Abs. 2 BetrVG muss daher klargestellt werden, dass der Anwendungsbereich die Verarbeitung personenbezogener Daten nicht umfasst, falls ein Datenschutzbeauftragter bestellt ist. Dies würde auch zu einer Entlastung der Betriebsräte führen und den Konflikt mit den Datenschutzbeauftragten auflösen. Deutschland ist eines der wenigen Länder, das von der Ermächtigung Gebrauch

gemacht hat, die Bestellung eines Datenschutzbeauftragten ab einer bestimmten Anzahl von Mitarbeitenden, die personenbezogene Daten verarbeiten, verpflichtend vorzuschreiben. Der positive Effekt hiervon wird allerdings dann nicht erreicht, wenn der Gesetzgeber Kontrollinstanzen konkurrieren lässt.

Mehr Klarheit für kollektivrechtliche Regelungen

Die Einbeziehung von Kollektivvereinbarungen zur Konkretisierung des Beschäftigtendatenschutzes funktioniert in der Praxis bereits sehr gut. Bei dem Vorschlag einer gesetzlichen Konkretisierung für solche Vereinbarungen ist zu beachten, dass diese Vereinbarungen einen Ausgleich zwischen den beiderseitigen Interessen schaffen müssen. Ein gesetzlicher Rahmen könnte die Handlungsmöglichkeiten einschränken und den Ausgleich gefährden.