bitkom

Stellungnahme

Januar 2025

Bitkom zum Referentenentwurf eines Beschäftigtendatengesetzes

Zusammenfassung

Im Oktober 2024 ist der Entwurf eines Gesetzes zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (Beschäftigtendatengesetz) bekannt geworden.

Bitkom nimmt zum aktuellen Entwurf des Beschäftigtendatengesetzes (BeschDG-E) wie folgt Stellung:

1. Der Gesetzentwurf ist in vielen Bereichen zu rigoros und bürokratisch, was die Flexibilität und Handlungsfähigkeit der Unternehmen einschränkt und Innovationsprozesse behindert. Insbesondere in den Bereichen Erforderlichkeit, Zweckbindung, Überwachung und KI-Nutzung, könnten Unternehmen nicht nur mit erheblichem Verwaltungsaufwand belastet, sondern auch in ihrer Flexibilität bei der Datenverarbeitung unnötig eingeschränkt werden.

2. Einige Neuregelungen im allgemeinen Teil erhöhen den bürokratischen Aufwand in Unternehmen, ohne dabei den Schutz der Beschäftigten tatsächlich zu erhöhen. Insbesondere die Auflistung von Punkten, die bei der Erforderlichkeitsprüfung oder bei Schutzmaßnahmen zugunsten der Beschäftigten beachtet werden sollen, führen zu weitergehenden Dokumentationspflichten. Außerdem werden die Auskunftspflichten deutlich erweitert.

3. Arbeitgeber könnten künftig unter Umständen nicht mehr auf Art. 6 Abs. 1 lit. f DS-GVO zurückgreifen, sofern spezifische Regelungen des BeschDG-E Anwendung finden. Dies würde die bisherige Flexibilität bei der Verarbeitung von Beschäftigtendaten erheblich einschränken und die Nutzung des „berechtigten Interesses“ als Grundlage für zahlreiche datengetriebene Prozesse deutlich reduzieren.

4. Der Entwurf berücksichtigt nicht hinreichend, dass nationale Regelungen im Beschäftigtendatenschutz immer die europäische Perspektive und den Harmonisierungsgedanken der DS-GVO im Blick haben sollten. Einige Regelungen führen daher zu Doppelregelungen oder stehen im Widerspruch zum EU-Recht.

5. Der Gesetzentwurf sieht ein Mitbestimmungsrecht des Betriebsrats bei der Benennung und Abberufung von Datenschutzbeauftragten vor (§ 12 BeschDG-E). Diese Regelung birgt erhebliche rechtliche und praktische Probleme, da sie die Entscheidungsfreiheit des Arbeitgebers einschränkt, die Unabhängigkeit des Datenschutzbeauftragten gefährdet und nicht im Einklang mit den Vorgaben der DS-GVO steht. Zudem kann sie insbesondere in global agierenden Unternehmen zu Konflikten, Verzögerungen und organisatorischen Schwierigkeiten führen. Ein Informations- oder Anhörungsrecht des Betriebsrats wäre hier eine angemessenere Alternative, die sowohl die Unabhängigkeit des Datenschutzbeauftragten als auch die Gestaltungshoheit des Arbeitgebers wahrt.

6. Zudem wird nicht berücksichtigt, dass bei Konzernen viele Personalprozesse einheitlich von einer Gesellschaft für mehrere andere Gesellschaften in verschiedenen Ländern erbracht werden. Nationale Sonderreglungen stehen dem entgegen und erhöhen Aufwand und Komplexität.

Im Einzelnen

Grundlagen der Datenverarbeitung (§ 3 BeschDG-E)

Positiv zu bewerten ist, dass der Entwurf eine Klarstellung enthält, dass Datenverarbeitungen im Arbeitsverhältnis nicht ausschließlich auf vertragliche (absolut) erforderliche Zwecke beschränkt sind und z.B. auch eine Datenverarbeitung aufgrund berechtigter Interessen zulässig sein kann.

Der vorliegende Entwurf für § 3 BeschDG-E ist jedoch in mehreren Punkten kritisch zu bewerten, da er über die Vorgaben der DS-GVO hinausgeht, Rechtsunsicherheit schafft und in der Praxis nicht umsetzbare Hürden einführt.

Im Einzelnen:

1. **Zusätzliches Erfordernis des „Überwiegens der Interessen des Arbeitgebers“**
   Die Einführung des Kriteriums, dass die Interessen des Arbeitgebers überwiegen müssen, geht über die Anforderungen der DS-GVO hinaus. Das Kriterium der „Erforderlichkeit“ beinhaltet bereits eine Verhältnismäßigkeitsprüfung, bei der die Interessen der betroffenen Beschäftigten angemessen berücksichtigt werden.

   Das zusätzliche Merkmal des „Überwiegens“ verkompliziert die Rechtmäßigkeit der Datenverarbeitung erheblich und schafft ein Regel-Ausnahme-Verhältnis, das der DS-GVO fremd ist. Insbesondere für konkrete Fallkonstellationen wie die Feststellung der Eignung eines Beschäftigten für eine Tätigkeit ist das Merkmal nicht praktikabel.

Zudem widerspricht das zusätzliche Erfordernis den Prinzipien der DS-GVO, wonach die Beweislast für die Rechtmäßigkeit der Verarbeitung ohnehin beim Verantwortlichen liegt (Art. 5 Abs. 2, Art. 24 Abs. 1 DS-GVO). Es ist daher nicht erforderlich, die Interessen des Arbeitgebers explizit hervorzuheben.

Ein Vergleich mit § 24 Abs. 1 des Gesetzentwurfs zeigt, dass in bestimmten Fällen sogar ein „erhebliches" Überwiegen verlangt wird. Dies verdeutlicht, dass das „Überwiegen" eine zusätzliche Hürde darstellt, die über das Verhältnismäßigkeitsprinzip hinausgeht.

Das Kriterium des „Überwiegens der Interessen des Arbeitgebers" sollte durch die Formulierung „sofern nicht die Interessen des betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen" ersetzt werden, um die Praxisnähe und Rechtsklarheit zu gewährleisten. Alternativ sollte nur das Merkmal der „Erforderlichkeit" verlangt werden.

2. **Unklare Terminologie und Regelungsdichte in § 3 Abs. 1**
   Die Verwendung des Begriffs „konkrete" Zwecke weicht ohne Not von den Begrifflichkeiten der DS-GVO („eindeutige, legitime und festgelegte Zwecke") ab. Dies ist systemfremd, da die Öffnungsklausel des Art. 88 DS-GVO nur spezifischere Regelungen zulässt.

   Teilweise wiederholt Abs. 1 lediglich bestehende Regelungen aus Art. 6 DS-GVO, ohne eigenständigen Regelungsgehalt hinzuzufügen. Dies widerspricht der Rechtsprechung des EuGH zu § 26 Abs. 1 Satz 1 BDSG, der bereits eine Wiederholung bestehender DS-GVO-Regelungen kritisiert hat.

   Die Formulierungen sollten an die Begriffe und Vorgaben der DS-GVO angepasst werden, um Unklarheiten und Widersprüche zu vermeiden.

3. **Systemfremde Elemente in § 3 Abs. 3 und Abs. 4**
   § 3 Abs. 3 wiederholt Grundprinzipien der DS-GVO, insbesondere die Zweckbindung. Der Zweck einer Verarbeitung allein ist jedoch nicht ausreichend, um deren Rechtmäßigkeit zu beurteilen.

   Die Auflistung spezifischer Daten wie Name oder Bankverbindung ist im Datenschutzrecht unüblich und problematisch (vgl.§ 3 Abs. 4). Sie greift der im Einzelfall erforderlichen Prüfung von Erforderlichkeit und Datenminimierung vor und setzt einen unnötig detaillierten Maßstab. Zudem ist es offensichtlich, dass die Verarbeitung einer Bankverbindung für die Gehaltsauszahlung erforderlich ist – dies bedarf keiner gesetzgeberischen Regelung.

   Die Wiederholung der Grundprinzipien der DS-GVO in Abs. 3 und die Regelungstiefe von Abs. 4 sollten gestrichen oder deutlich reduziert werden. Es ist nicht notwendig, offensichtliche Verarbeitungszwecke wie die Gehaltszahlung auf gesetzlicher Ebene zu regeln. Absatz 3 kann zudem eine massive Erhöhung des Dokumentationsaufwands bedeuten.

4. **Praktische Probleme durch starre Anforderungen**
   Die Vorgabe, dass die Interessen des Arbeitgebers oder des Konzerns überwiegen müssen, erschwert einfache und notwendige Prozesse wie konzerninternes

Recruiting erheblich. Mitarbeiter-Einwilligungen sind in der Praxis nicht praktikabel, da sie hohen Aufwand bedeuten und oft nicht zielführend sind.

Beispiel: Wenn ein Konzernunternehmen nach qualifizierten Mitarbeitern für eine Stelle sucht, sollten zunächst Qualifikationen oder Vergütungsbestandteile ausgetauscht werden können, um die Realisierbarkeit zu prüfen. Eine solche Datenverarbeitung wird durch die aktuellen Regelungen unangemessen erschwert.

Fazit: Die Kombination von „Erforderlichkeit“ und „Überwiegen der Interessen des Arbeitgebers“ führt zu erheblicher Rechtsunsicherheit. Besonders in Bereichen mit klar definierten Zwecken (z.B. Eignungsfeststellung, Gehaltszahlung) ist diese zusätzliche Voraussetzung nicht nur unnötig, sondern kontraproduktiv. Der Fokus sollte auf der „Erforderlichkeit“ liegen, da diese bereits eine hinreichende Abwägung der Interessen sicherstellt. Konkretisierungen oder starre Regelungen wie die in Abs. 4 sollten vermieden werden, um unnötige Bürokratie zu reduzieren und die Einhaltung der Datenschutzprinzipien der DS-GVO zu gewährleisten. Diese Anpassungen sorgen für eine klare, praktikable und europarechtskonforme Regelung, die sowohl den Schutz der Beschäftigten als auch die berechtigten Interessen der Arbeitgeber berücksichtigt.

Prüfung der Erforderlichkeit (§ 4 BeschDG-E)

Der Gesetzentwurf sieht vor, dass bei jeder Verarbeitung von Beschäftigtendaten eine strenge Prüfung der Erforderlichkeit unter Berücksichtigung der dort genannten Kriterien erfolgen muss, wobei die Abhängigkeit der Beschäftigten im Arbeitsverhältnis besonders zu berücksichtigen ist.

Diese Regelung bedeutet mehr Begründungs- und Dokumentationsaufwand für Arbeitgeber als bislang und könnte dazu führen, dass Arbeitgeber übermäßig vorsichtig agieren und dadurch betriebsnotwendige Datenverarbeitungen unterlassen, aus Angst vor möglichen Sanktionen. Dies führt zu einem unnötigen bürokratischen Aufwand und könnte Innovationen behindern, da jeder Schritt einer Datenverarbeitung umfassend dokumentiert und begründet werden muss. Da entsprechende Prüf- und Dokumentationsanforderungen in der DS-GVO bereits niedergelegt sind, führen die Zusatzanforderungen zu einer Benachteiligung der deutschen Wirtschaft im europäischen Vergleich.

§ 4 Nr. 2 lit. g BeschDG-E lässt den früher geltenden Grundsatz der Direkterhebung wieder aufleben. Dieser Grundsatz existiert jedoch in der DS-GVO nicht mehr und sollte auch über das Beschäftigtendatenschutzgesetz nicht wieder ins Leben gerufen werden. Die DS-GVO regelt bereits ausreichend, welche Daten wann auf welche Weise verarbeitet werden dürfen. Die Daten müssen nicht immer zwingend bei dem Betroffenen direkt erhoben werden.

Hinsichtlich § 4 Nr. 2 lit. i BeschDG-E ist zu sagen, dass eine möglicherweise zweckwidrige Verarbeitung in der Erforderlichkeitsprüfung keine Rolle spielen kann. Streng genommen könnten dann viele Datenverarbeitungsvorgänge an diesem Abwägungsaspekt scheitern. Wenn ein Mitarbeiter Daten rechtswidrig verarbeitet,

kann dies entsprechende arbeitsrechtliche Konsequenzen haben. Einer Regelung an dieser Stelle bedarf es jedoch nicht.

Einwilligung (§ 5 BeschDG-E)

§ 5 BeschDG-E regelt die Einwilligung und die damit im Zusammenhang stehende Problematik der Freiwilligkeit einer Einwilligung zur Datenverarbeitung während und nach Durchführung eines Beschäftigungsverhältnisses.

Die Regelungen zur Einwilligung der Betroffenen im Beschäftigungsverhältnis werden unnötig detailliert. Dies wird in der Praxis zu weiteren Prüf- und Dokumentationsanforderungen führen und damit zu einem nicht unerheblichen Zusatzaufwand. Da entsprechende Anforderungen in der DS-GVO bereits niedergelegt sind, führen die Zusatzanforderungen zu einer Benachteiligung der deutschen Wirtschaft im europäischen Vergleich.

Besondere Kategorien von Beschäftigtendaten (§ 6 BeschDG-E)

Die ausdrückliche Aufnahme der Interessenabwägung bei der Datenverarbeitung von besonderen Kategorien von personenbezogenen Daten, die der Ausübung oder Erfüllung von durch Rechtsvorschrift oder Kollektivvereinbarung festgelegten Rechten oder Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes dienen, würde im Umkehrschluss bedeuten, dass es Fälle geben würde, in denen das Unternehmen seine Pflichten aus dem Gesetz oder Kollektivvereinbarungen nicht erfüllen könnte und damit also faktisch einen Rechtsbruch erfüllen würde, weil Rechte der Betroffenen entgegen stehen.

Demgemäß darf der Teilsatz in § 6 Abs 1 „...und dabei die Interessen des Arbeitgebers an der Verarbeitung die Interessen der betroffenen Beschäftigten an dem Ausschluss der Verarbeitung überwiegen“ nicht bestehen bleiben. Eine Interessenabwägung ist bei der Erfüllung von Rechtspflichten fehl am Platz.

Kollektivvereinbarungen (§ 7 BeschDG-E)

Entgegen der bisherigen Rechtslage in § 26 Abs. 2 BDSG soll die Verarbeitung von Beschäftigtendaten nicht mehr auf Kollektivvereinbarungen als Rechtsgrundlage gestützt werden können. Damit wird Unternehmen und Sozialpartnern die Möglichkeit genommen, sich an betrieblichen Bedürfnissen orientierende Rechtsgrundlagen für Datenverarbeitungen zu schaffen.

Verarbeitung zu anderen Zwecken (§ 8 BeschDG-E)

Zwar ist positiv zu bewerten, dass es eine Regelung zur Weiterverarbeitung von Daten zu anderen Zwecken gibt; allerdings kann diese Befugnis ebenfalls bereits über die DS-GVO hergeleitet werden und ist daher überflüssig. Im Kontext der Weiterverarbeitung besteht auch Anpassungsbedarf bei § 23 BeschDG-E, der die Zweckänderung von bereits erhobenen Daten zum Zwecke der Leistungskontrolle ausschließt bzw. unnötig

erschwert. Es ist aber auch im Interesse der Beschäftigten, Daten zur Leistungsbeurteilung nicht noch einmal zusätzlich erheben zu müssen. Also muss eine Regelung gefunden werden, die die Weiterverarbeitung unter bestimmten Umständen ermöglicht.

Schutzmaßnahmen (§ 9 BeschDG-E)

Arbeitgeber müssen umfassende technische und organisatorische Maßnahmen zum Schutz der Daten treffen, einschließlich besonderer Vorkehrungen für KI-Systeme.

Eine ergänzende Regelung ist aus Sicht des Bitkom nicht erforderlich, da in der DS-GVO bereits ausreichende Regelungen vorhanden sind, die sich in der Praxis bewährt haben.

Die Anforderungen an technische und organisatorische Schutzmaßnahmen im Zusammenhang mit KI und deren Protokollierung können insbesondere für kleine und mittelständische Unternehmen (KMU) schwer umsetzbar und kostspielig sein. Der Aufwand für die Implementierung und regelmäßige Überprüfung dieser Maßnahmen steht nicht im Verhältnis zu den tatsächlichen Risiken und Bedürfnissen des Unternehmens, zumal man nicht per se sagen kann, dass KI-Systeme datenschutzrechtlich riskanter sind als IT-Systeme.

Zudem kann die Pflicht, über die getroffenen Schutzmaßnahmen Auskunft zu erteilen dazu führen, dass Informationen über die betriebliche Sicherheit oder Betriebs- und Geschäftsgeheimnisse offengelegt werden müssen. Auch in diesem Kontext ist eine starke Benachteiligung der deutschen gegenüber der europäischen Wirtschaft zu befürchten.

Gleiches gilt für die Schutzmaßnahmen zur Verarbeitung von Beschäftigtendaten beim Einsatz einer Künstlichen Intelligenz (§ 9 Abs. 1 Ziff.11, Abs. 2 und 3 BeschDG-E). Die Regelungen zu KI-Systemen führen vor allem zu einer Doppelung zur europäischen Regelung und damit zu nicht tragbaren Rechtsunsicherheiten. Hier muss die KI-Verordnung die führende Regelung bleiben.

Spezifische Betroffenenrechte (§ 10 BeschDG-E)

Arbeitgeber müssen auf Verlangen der Beschäftigten die wesentlichen Erwägungen der Interessenabwägung bei der Datenverarbeitung darlegen.

Diese Pflicht könnte einen erheblichen Verwaltungsaufwand verursachen, insbesondere in großen Unternehmen mit vielen Beschäftigten. Arbeitgeber könnten gezwungen sein, umfangreiche Dokumentationen zu erstellen, um auf mögliche Anfragen vorbereitet zu sein, was ineffizient ist und Ressourcen bindet.

Zudem gehen § 10 Abs. 2 und 3 über die Vorgaben der KI-Verordnung hinaus und schaffen Doppelregulierung. Es ist nicht ersichtlich, warum gesonderte Informationspflichten und Auskunftsrechte für KI-Systeme eingeführt werden sollen, die nicht in den Hochrisiko-Bereich fallen. Der Gesetzgeber sollte nicht pauschal davon ausgehen, dass KI-Systeme datenschutzrechtlich riskanter sind als IT-Systeme.

Die Regelungen zu den Auskunftsrechten und Informationspflichten in den §§ 10, 25 und 26 sind komplex, ineinander verschachtelt und stehen teilweise neben den Rechten aus der DS-GVO („unbeschadet“). Dies erhöht den Aufwand und die Fehleranfälligkeit.

Verwertungsverbot (§ 11 BeschDG-E)

Datenschutzrechtswidrig verarbeitete Daten dürfen grundsätzlich nicht in gerichtlichen Verfahren gegen Beschäftigte verwendet werden. Ein Verwertungsverbot kann in Kollektivvereinbarungen vereinbart werden.

Das entspricht faktisch einem Beweisverwertungsverbot und widerspricht dem bisher anerkannten Grundsatz, dass die Entscheidung über die Zulässigkeit der Beweismittel dem jeweiligen Richter obliegt. Die Möglichkeit zur Aufnahme eines Verwertungsverbots in Kollektivvereinbarungen wird dazu führen, dass künftig jeder Betriebsrat dies verlangt.

Mitbestimmung bei Datenschutzbeauftragten (§ 12 BeschDG-E)

Der Betriebsrat hat ein Mitbestimmungsrecht bei der Benennung und Abberufung von Datenschutzbeauftragten.

Die Regelung, dem Betriebsrat ein Mitbestimmungsrecht bei der Benennung und Abberufung von Datenschutzbeauftragten (DSB) einzuräumen, birgt erhebliche rechtliche und praktische Probleme. Sie greift unverhältnismäßig in die Gestaltungshoheit des Arbeitgebers ein und steht teilweise im Widerspruch zu den Vorgaben der DS-GVO.

Im Einzelnen:

1. **Einschränkung der betrieblichen Entscheidungsfreiheit**
   Der DSB berät und überwacht den Arbeitgeber bei der Einhaltung der Datenschutzvorschriften (Art. 39 DS-GVO). Der Arbeitgeber ist als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO für die Verarbeitung personenbezogener Daten verantwortlich und trägt die alleinigen Pflichten und Sanktionen gemäß DS-GVO und BDSG. Daher muss er auch allein über die Eignung und den Einsatz des DSB entscheiden können. Das Mitbestimmungsrecht des Betriebsrats schränkt diese Entscheidungsfreiheit ein und kann zu erheblichen Verzögerungen führen, wenn keine Einigung mit dem Betriebsrat erzielt wird. Eine Einigungsstelle könnte notwendig werden, was dazu führen kann, dass zeitweise kein DSB benannt ist.

2. **Gefährdung der Unabhängigkeit des Datenschutzbeauftragten**
   Der DSB muss neutral und unabhängig agieren (Art. 37 Abs. 5 DS-GVO), auch gegenüber dem Betriebsrat. Ein Mitbestimmungsrecht könnte jedoch dazu führen, dass der DSB nach Kriterien ausgewählt wird, die den Interessen des Betriebsrats entsprechen, etwa Gewerkschaftszugehörigkeit. Gleichzeitig ist der DSB verpflichtet, den Betriebsrat in Datenschutzfragen zu überwachen. Diese Doppelfunktion kann problematisch werden, wenn der DSB von der Zustimmung

des Betriebsrats abhängig ist. Die Unabhängigkeit des DSB würde erheblich beeinträchtigt.

3. **Missverhältnis zwischen Beschäftigten- und Kundendaten**
   Die Regelung verkennt, dass Unternehmen nicht nur Beschäftigtendaten, sondern oft eine wesentlich größere Menge an Kundendaten verarbeiten. Die datenschutzrechtliche Verantwortung für Kundendaten würde durch das Mitbestimmungsrecht des Betriebsrats unverhältnismäßig beeinträchtigt.

4. **Benachteiligung global agierender Unternehmen**
   Die Regelung berücksichtigt nicht die Anforderungen global oder europaweit agierender Unternehmen. Ein konzernweiter DSB gemäß Art. 37 Abs. 2 DS-GVO könnte nicht ohne Zustimmung des deutschen Betriebsrats benannt werden, selbst wenn er für Standorte außerhalb Deutschlands verantwortlich ist. Dies widerspricht den Harmonisierungsvorgaben der DS-GVO und benachteiligt international tätige Unternehmen erheblich.

5. **Konfliktpotenzial bei Abberufungen**
   Auch bei der Abberufung eines DSB gemäß Art. 37 Abs. 5 und 6 DS-GVO könnten Konflikte entstehen, wenn der Betriebsrat Mitbestimmungsrechte hat. Notwendige Maßnahmen, etwa bei mangelnder Eignung des DSB, könnten durch Betriebsratswiderstand verzögert oder verhindert werden.

6. **Gefahr eines „Stillstands“ bei Verweigerungshaltung des Betriebsrats**
   Ein Arbeitgeber könnte auf die Zustimmung eines mit ihm in Konflikt stehenden Betriebsrats angewiesen sein. Dies kann dazu führen, dass längere Zeit kein DSB benannt wird oder ein durch die Einigungsstelle verordneter DSB eingesetzt wird. Letzteres würde die Gestaltungshoheit des Arbeitgebers erheblich beeinträchtigen.

7. **Missbrauchsrisiken und Parallelstrukturen**
   Betriebsratsgremien könnten versuchen, eigene DSB zu benennen, um den betrieblichen DSB zu blockieren oder nach eigenen Präferenzen auszuwählen. Dies widerspricht den Anforderungen der DS-GVO an die Qualifikation und Neutralität des DSB (Art. 37 Abs. 5 DS-GVO) und führt zu organisatorischen Konflikten.

8. **Kompetenzüberschreitung durch zusätzliche Anforderungen bei der Benennung**
   Artikel 37 Absatz 4 Satz 1 Halbsatz 2 DS-GVO überlässt den Mitgliedsstaaten zwar die Benennung weiterer Benennungstatbestände. Nicht in die Kompetenz der Mitgliedstaaten fällt aber die Kompetenz, eine Benennung an Zustimmungserfordernisse Dritter zu knüpfen.

   Fazit: Die Benennung und Abberufung von Datenschutzbeauftragten sollten nicht der Mitbestimmung des Betriebsrats unterliegen. Stattdessen könnte ein Informations- oder Anhörungsrecht des Betriebsrats eingeführt werden.

   Dadurch:

   a) bliebe die Unabhängigkeit des DSB gewahrt,

   b) würde die Gestaltungshoheit des Arbeitgebers gesichert,

   c) würden Konflikte und Verzögerungen vermieden,

d) bliebe die Europarechtskonformität der Regelung gewährleistet.

Dieses Modell bietet eine angemessene Beteiligung des Betriebsrats, ohne die datenschutzrechtliche Verantwortlichkeit und Compliance des Arbeitgebers zu gefährden.

Eignungsfeststellung (§ 13 BeschDG-E)

Die Verarbeitung von vom Bewerber öffentlich zugänglich gemachten Daten (z.B. Social Media) muss zur Entscheidung über die Begründung eines Beschäftigungsverhältnisses weiterhin zulässig und praktisch durchführbar bleiben. Die inhaltlich und zeitlich deutlich über die DS-GVO hinausgehenden Informationspflichten aus § 25 BeschDG-E vor Verarbeitung von Bewerberdaten aus z.B. Social Media erschweren diese Verarbeitung deutlich und gehen an der Lebensrealität vorbei.

Berufliche Netzwerke wie LinkedIn oder XING haben den Zweck berufliche Qualifikationen und Informationen zu teilen, die für eine Bewerbung relevant sein könnten. Da die Bewerber diese Informationen freiwillig zu diesen Zwecken öffentlich machen, besteht der im § 25 BeschDG-E festgelegte, über die DSGVO hinausgehende, Informations- und Schutzbedarf nicht.

Positive Maßnahmen (§ 15 BeschDG-E)

Diese Regelung würde die Bewerber in gewisser Weise „bevormunden“. Wenn sie freiwillig Daten zur Verfügung stellen, muss das Unternehmen diese auch weiterhin verarbeiten dürfen.

Löschpflichten (§ 17 BeschDG-E)

Daten, die vor der Begründung eines Beschäftigungsverhältnisses verarbeitet wurden, müssen spätestens drei Monate nach Ablehnung des Bewerbers gelöscht werden.

Die im Gesetz vorgesehene starre Frist von drei Monaten zur Löschung von Daten abgelehnter Bewerber wirft erhebliche praktische, rechtliche und organisatorische Bedenken auf:

1. **Abweichung von der bisherigen Rechtsprechung**
   Bislang wurde eine Speicherung von fünf bis sechs Monaten nach Ablehnung von der Rechtsprechung anerkannt, um die dreimonatige Klagefrist nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) und die Zustellzeit für Klagen an den Arbeitgeber abzudecken. Die Reduktion auf drei Monate widerspricht der etablierten Praxis und den Anforderungen an eine angemessene Dokumentation, sollte es zu rechtlichen Auseinandersetzungen kommen.

2. **Unvereinbarkeit mit marktüblichen Tools und Prozessen**
   Viele im Markt genutzte Bewerbermanagement-Systeme trennen zwischen Bewerberprofilen und spezifischen Bewerbungsdaten. Eine starre Dreimonatsfrist passt nicht zu den automatisierten Routinen dieser Systeme und erschwert die

Umsetzung standardisierter Löschprozesse erheblich. Unternehmensintern sind häufig Löschläufe für vier oder sechs Monate nach Ablehnung vorgesehen, was auf die etablierten rechtlichen Rahmenbedingungen abgestimmt ist.

3. **Eingriff in HR-Prozesse und EU-weite Einheitlichkeit**
   Die starre Löschfrist greift ohne sachlichen Grund in die HR-Prozesse und Löschroutinen von Unternehmen ein. Sie weicht zudem von den flexiblen Vorgaben der DS-GVO zur Speicherbegrenzung ab, die eine Speicherung so lange erlauben, wie ein berechtigter Zweck (hier die Abwehr potenzieller Klagen) besteht. Eine flexible Formulierung wie „innerhalb einer angemessenen Frist“ wäre mit der DS-GVO konform und würde eine einheitliche Handhabung in der EU ermöglichen.

4. **Unverhältnismäßigkeit der Löschpflicht bei zurückgezogenen Bewerbungen**
   Die Verpflichtung zur „unverzüglichen Löschung“ bei zurückgezogenen Bewerbungen (Abs. 1, S. 3) ist in der Praxis kaum umsetzbar. Auch hier könnten Rechtsstreitigkeiten, etwa bei mutmaßlichem Missbrauch oder Diskriminierungsansprüchen, auftreten. Eine „angemessene Frist“ für die Löschung sollte auch in diesen Fällen vorgesehen werden, um eine sachgerechte Abwicklung zu ermöglichen.

   Fazit: Die Löschfrist für Bewerberdaten sollte nicht starr auf drei Monate begrenzt werden. Stattdessen sollte die Formulierung „innerhalb einer angemessenen Frist“ eingeführt werden, die sich an den Vorgaben der DS-GVO zur Speicherbegrenzung orientiert. Für zurückgezogene Bewerbungen sollte ebenfalls eine angemessene Frist definiert werden, um potenziellen Rechtsstreitigkeiten Rechnung zu tragen und die Praktikabilität in der Umsetzung sicherzustellen.

   Dieses Vorgehen gewährleistet eine praktikable und rechtssichere Umsetzung für Unternehmen und sichert gleichzeitig die Einhaltung der Datenschutzvorgaben.

Überwachung von Beschäftigten (§ 18 BeschDG-E)

Bei dieser Regelung drohen Abgrenzungsschwierigkeiten zur datenschutzrechtlich notwendigen dauerhaften Protokollierung von Verarbeitungen personenbezogener Daten (z. B. durch Mitarbeiter von HR oder im Kundenservice) – diese Datenschutzkontrolle darf keinesfalls nur anlassbezogen oder stichprobenartig erfolgen; dies wäre ein klarer Verstoß gegen Art. 32 DSGVO (Aufsichtsbehörden verlangen regelmäßig den Nachweis der Protokollierung der Datenverarbeitung).

Nicht nur kurzzeitige Überwachungsmaßnahmen (§ 19 BeschDG-E)

Nicht nur kurzzeitige Überwachungsmaßnahmen sind nur in engen Ausnahmefällen zulässig, wenn sie z. B. Leib und Leben schützen sollen.

Diese Vorschrift engt die Handlungsspielräume der Arbeitgeber erheblich ein, wenn es um die kontinuierliche Überwachung aus berechtigten Interessen (z. B. Schutz von Eigentum oder sensiblen Daten) geht, die wohl nicht immer die Anforderungen

erfüllen, insbesondere in Bezug auf die erhebliche Überwiegung der Arbeitgeberinteressen.

Videoüberwachung (§ 21 BeschDG-E)

Die starre Löschfrist von 72 Stunden weicht ohne sachlichen Grund von den Vorgaben der DS-GVO zur Speicherbegrenzung ab und erschwert einheitliche HR-Prozesse in der EU.

Ortung (§ 22 BeschDG-E)

Die nicht nur kurzfristige Ortung von Beschäftigten ist nur unter strengen Voraussetzungen zulässig, insbesondere müssen die Arbeitgeberinteressen die Interessen der Arbeitnehmer erheblich überwiegen.

Die Regelungen zur Ortung von Beschäftigten, insbesondere die geplante Einschränkung oder gar ein Verbot, sind aus Arbeitgebersicht problematisch, da sie die betriebliche Effizienz, Transparenz und Sicherheit erheblich beeinträchtigen könnten. In vielen Arbeitsbereichen, insbesondere der Logistik, ist die Ortung unverzichtbar, um Lieferprozesse effizient zu planen, Verzögerungen zu vermeiden und Kunden genaue Informationen über Lieferzeiten zu bieten. Ein vollständiges Verbot würde zu Ineffizienzen, längeren Lieferzeiten, höheren Kosten und einer Beeinträchtigung der Wettbewerbsfähigkeit führen, insbesondere im internationalen Vergleich.

Die Regelung, dass eine Interessenabwägung erforderlich ist, selbst wenn die Ortung durch kollektivrechtliche Vereinbarungen gedeckt ist, stellt einen zusätzlichen bürokratischen Aufwand dar und entwertet bestehende Vereinbarungen, die bereits eine Interessenabwägung beinhalten. Dies widerspricht dem Grundsatz der Praxisnähe und führt zu einer unnötigen Doppelprüfung.

Darüber hinaus ist die Ortung auch ein wesentlicher Sicherheitsfaktor, sowohl für die Ware als auch für die Beschäftigten. In Fällen von Diebstahl, Verlust oder Gefahrensituationen kann die Verortung entscheidend sein, um Schäden zu verhindern oder einzudämmen. Bereits die DS-GVO regelt umfassend, unter welchen Bedingungen die Ortung zulässig ist. Eine weitere Einschränkung geht über die bestehenden Regelungen hinaus und gefährdet die Praxisfähigkeit moderner Arbeitsprozesse.

Eine stärkere Berücksichtigung betrieblicher Notwendigkeiten ist erforderlich, wobei ein Überwiegen der Arbeitgeberinteressen gegenüber den Interessen der Arbeitnehmer als ausreichend angesehen werden sollte.

Leistungskontrolle (§ 23 BeschDG-E)

Die Datenverarbeitung zur Leistungskontrolle soll weitestgehend verboten werden.

Die derzeit vorliegende Formulierung legt nahe, dass eine Datenverarbeitung entweder gar nicht oder nicht „auch" zum Zwecke einer notwendigen Leistungskontrolle möglich ist. Für die Zulässigkeit von Leistungskontrollen am

Arbeitsplatz gelten jedoch ohnehin bereits sehr hohe Anforderungen und Auflagen in Deutschland. Es besteht das Risiko für Unternehmen, dass notwendige Daten von Beschäftigten zum Zweck der Steuerung/Durchführung von Arbeitsprozessen nicht mehr verarbeitet werden können, da dies unmittelbar oder mittelbar als Leistungskontrolle gelten würde. Das birgt ein enormes Risiko für Logistikcenter und Logistikprozess, aber auch für andere Arbeitsbereiche in der modernen Arbeitswelt. Es würde stark einschränken, wie Logistikprozesse gesteuert werden (bspw. Schichtpläne, Einteilung, Verschiebung von Arbeitskräften), weil nicht berücksichtigt werden darf, welcher Mitarbeitende für welche Arbeitsprozesse geeignet ist und eingesetzt werden kann. Auch die gezielte und in der komplexen Arbeitswelt notwendige Entwicklung der Arbeitnehmenden wird dadurch stark eingeschränkt. Deutschland ist aufgrund seiner geografischen Lage ein sehr wichtiger Standort für Logistikunternehmen angrenzende Branchen – Deutschland ist das Logistikzentrum Europas. Es darf nicht unterschätzt werden, dass dieser Vorschlag dem Standort Deutschland schaden und den Standortvorteil aufs Spiel setzen würde.

Es sollte eine klare Abgrenzung zwischen der reinen Leistungskontrolle und der notwendigen Steuerung von Arbeitsprozessen geben. Jedoch nicht wie vorgeschlagen anhand der Datenverarbeitung oder einer anderen Zwecke ausschließenden, einmaligen Zweckbindung/Zwecksperre, sondern anhand der erforderlichen Prozesse. Die Steuerung von Beschäftigten in komplexen Arbeitsprozessen geht weit über die Organisation von Schichtplänen und die effiziente Zuweisung von Aufgaben hinaus. Sie ist essenziell, um Arbeitsabläufe in Logistikprozessen zu gewährleisten und damit für die Durchführung des Arbeitsverhältnisses. Ohne eine Datenauswertung könnten diese Prozesse kaum oder nicht mehr durchgeführt werden.

Die Einschränkung der Datenverarbeitung über die bereits anspruchsvollen Regelungen der DS-GVO hinaus, könnte zu massiven Ineffizienzen führen, insbesondere in der Hochsaison des Onlinehandels, in der eine präzise Planung entscheidend ist. Ein Verbot der Nutzung von Daten zur Steuerung und Optimierung könnte die Wettbewerbsfähigkeit deutscher Logistikunternehmen gefährden.

Eine differenzierte Betrachtung der Arbeitsleistung trägt gerade auch dazu bei, Mitarbeitende gemäß ihren individuellen Fähigkeiten und Stärken dort einzusetzen, wo sie effizient sind und auch schwerer ersetzbar, was sowohl die Produktivität erhöht als auch die Zufriedenheit der Beschäftigten und deren Sicherheit für den Arbeitsplatz fördern kann. Ein pauschales Verbot der Leistungskontrolle würde diese Möglichkeit stark einschränken.

Deutschland als Logistikzentrum Europas hängt maßgeblich von der Effizienz seiner Prozesse ab. Internationale Partner und Kunden erwarten Zuverlässigkeit und Präzision. Restriktionen bei der Datennutzung könnten das Vertrauen in die Leistungsfähigkeit deutscher Logistikzentren und die deutsche Zuverlässigkeit als Qualitätskriterium untergraben.

Informationspflicht bei Profiling (§ 25 BeschDG-E)

Arbeitgeber müssen Beschäftigte über den Einsatz von Profiling ausführlich informieren.

Diese umfangreichen Informationspflichten gehen deutlich über die der DS-GVO hinaus und können in der Praxis schwer umsetzbar sein und zu zusätzlichem bürokratischen Aufwand führen.

Auskunftsrecht bei Profiling (§ 26 BeschDG-E)

Beschäftigte haben ein Recht auf detaillierte Auskunft über die Eingabedaten und die Ergebnisse des Profilings.

Diese Regelung könnte zu einer Flut von Anfragen und einem hohen administrativen Aufwand führen, da Arbeitgeber verpflichtet sind, detaillierte Auskünfte über komplexe Systeme zu erteilen. Auch hier wird weit mehr verlangt als es die DS-GVO vorsieht.

Erklärung und Überprüfung der Entscheidung (§ 27 BeschDG-E)

Beschäftigte haben das Recht, eine Erklärung und Überprüfung von Entscheidungen zu verlangen, die auf einem Profiling beruhen.

Diese Regelung könnte zu einer deutlichen Erhöhung des administrativen Aufwands führen, da jede Entscheidung, die auf automatisierten Verfahren beruht, von einer natürlichen Person überprüft und erklärt werden muss. Dies könnte den Einsatz moderner KI-Systeme zur Effizienzsteigerung behindern, da der Prozess der Entscheidungsfindung durch menschliches Eingreifen verlangsamt wird.

Darüber hinaus regelt § 27 in Absatz 2 einen neuen eigenen datenschutzrechtlichen Anspruch für Beschäftigte gerichtet auf die Abgabe einer eigenen Stellungnahme, Überprüfung der Entscheidung durch den Arbeitgeber und Erhalt einer begründeten Antwort innerhalb von 4 Wochen. Dieser Regelungsentwurf, sollte er unverändert in Kraft treten, birgt ein enormes Risiko für Arbeitgeber insofern, als dass mit der Geltendmachung dieses Anspruchs Beschäftigte versuchen können, v.a. im Rahmen von Kündigungsstreitigkeiten Druck auf den Arbeitgeber auszuüben. Auf diese Weise würde zusätzlich zu dem bereits bestehenden Auskunftsanspruch nach Art. 15 DS-GVO eine weitere massive Belastung des Arbeitgebers entstehen.

Datenverarbeitung zu Autorisierungs- und Authentifizierungszwecken (§ 28 BeschDG-E)

Die zusätzlichen Schutzmaßnahmen bei der Verwendung von biometrischen Daten im Rahmen der Datenverarbeitung zu Autorisierungs- und Authentifizierungszwecken sind in dieser Form teilweise nicht umsetzbar. Die Systeme, die für die Registrierung der Nutzer und deren biometrischen Daten zuständig sind, müssen in der Lage sein, z.B. eine Zugangsberechtigung gegen die hinterlegten Daten zu prüfen. Dies schließt die alleinige Verfügungsgewalt des Beschäftigten über das Speichermedium aus.

Betriebliches Eingliederungsmanagement (§ 29 BeschDG-E)

Das Schriftformerfordernis bei der Einwilligung sollte im Interesse des Arbeitnehmers an einer zügigen Durchführung des BEM und zur Vermeidung weiterer Bürokratie gestrichen werden.

Darüber hinaus ist die 24-Stunden-Frist aus Abs. 2 als nicht zielführend anzusehen. Unter der Prämisse, dass ein betriebliches Eingliederungsmanagement zugunsten des Betroffenen möglichst zügig durchgeführt werden sollte, würde diese 24-Stunden-Frist den Prozess nur verlangsamen. Zudem stellt sich die Frage, wie das Einhalten dieser Frist im Nachhinein geprüft/dargelegt/bewiesen werden soll. Eine solche weitere gesetzliche Hürde ist abzulehnen. Die Pflicht zur getrennten Aktenführung (Abs. 4) entspricht bereits der derzeitigen Rechtslage. Es ist jedoch hervorzuheben, dass die Tatsache, dass ein betriebliches Eingliederungsmanagement angeboten, durchgeführt und beendet wurde – ohne Inhalte dazu – weiterhin auch Gegenstand der Personalakte sein muss.

Datenverarbeitung im Konzern (§ 30 BeschDG-E)

Die Regelungen zur Datenverarbeitung im Konzern (§ 30 BeschDG-E) sind in ihrer aktuellen Form unzureichend, um die gestiegenen Anforderungen an moderne, agile Arbeitsstrukturen und Matrix-Organisationen innerhalb von Konzernen abzubilden. Die Regelung birgt Rechtsunsicherheiten und stellt praxisferne Anforderungen, die die konzerninterne Organisation erschweren.

Im Einzelnen:

1. **Unzureichende Rechtsklarheit bei konzerninternen Datenübermittlungen**
   Der Entwurf verfolgt das Ziel, Rechtsunsicherheiten bei konzerninternem Datentransfer zu beseitigen; erreicht dieses Ziel jedoch nicht. Insbesondere die Kombination aus dem Kriterium der „Erforderlichkeit“ und dem zusätzlichen Erfordernis eines „Überwiegens der Interessen des Arbeitgebers“ schafft zusätzliche Hürden. Beispielsweise bleibt unklar, ob und wie Bereiche wie Recruiting und Personalentwicklung von der Regelung erfasst sind. In der Praxis besteht ein erhebliches Interesse daran, qualifizierte Beschäftigte für Positionen in anderen Konzernteilen zu finden. Mitarbeiter-Einwilligungen sind dabei aufgrund des hohen Aufwands oder ihrer begrenzten Wirksamkeit nicht praktikabel.

2. **Einschränkung bei der Auftragsverarbeitung im Konzern**
   § 30 Abs. 3 erlaubt den systematischen Umkehrschluss, dass § 30 Abs. 1 auch dann gilt, wenn ein Konzernunternehmen als Auftragsverarbeiter für den Arbeitgeber tätig wird. Das bedeutet, dass die Datenverarbeitung innerhalb des Konzerns schlechter gestellt wird als die Nutzung eines externen Dienstleisters. Dies ist sachlich nicht gerechtfertigt und sollte explizit ausgeschlossen werden. Eine klare Regelung, dass § 30 Abs. 1 die Auftragsverarbeitung durch Konzernunternehmen nicht erfasst, ist notwendig, um praktische Umsetzungen und Effizienz in der Organisation zu gewährleisten.

3. **Unangemessene Einschränkung der bisherigen Rechtslage**
   Laut Gesetzesbegründung ist eine Offenlegung von Daten an weitere Konzernunternehmen explizit ausgeschlossen, selbst wenn sie erforderlich wäre, um konkrete Zwecke im Beschäftigungsverhältnis oder zur Wahrung berechtigter betrieblicher Interessen zu erreichen. Dies stellt eine unangemessene Verschärfung der bisherigen Rechtslage dar und behindert die effiziente Organisation von Konzernen, insbesondere in Branchen mit komplexen Anforderungen, wie dem Versicherungswesen (z.B. Spartentrennung nach Versicherungsaufsichtsrecht).

4. **Praktische Herausforderungen bei der Personalentwicklung und Recruiting**
   In vielen Fällen ist es für Personalentwicklung und Recruiting erforderlich, zunächst Qualifikationen und andere relevante Informationen (z.B. Vergütungsbestandteile) zwischen Konzernunternehmen auszutauschen, um potenzielle Kandidaten zu identifizieren. Diese Möglichkeiten werden durch die aktuellen Regelungen massiv eingeschränkt. Viele Mitarbeiter sind sich ihrer Entwicklungsmöglichkeiten im Konzern nicht bewusst, würden aber von konzernweiten Angeboten profitieren. Hier braucht es datenschutzkonforme, aber praktikable Regelungen, um diese Potenziale zu erschließen.

5. **Unnötige Benachteiligung von Konzernen mit komplexen Strukturen**
   Besonders Versicherungskonzerne mit Spartentrennung, aber auch andere Konzerne, in denen „shared services“ oder Matrix-Strukturen üblich sind, leiden unter der erschwerten Offenlegung von Beschäftigtendaten. Die Regelungen stellen einen Rückschritt dar und behindern die Agilität von Unternehmen, die ohnehin regulatorischen Anforderungen unterliegen.

   Fazit: Es sollte ausdrücklich geregelt werden, dass § 30 Abs. 1 keine Auftragsverarbeitung durch Konzernunternehmen erfasst. Die Notwendigkeit eines „Überwiegens der Interessen des Arbeitgebers“ sollte gestrichen werden. Das Kriterium der „Erforderlichkeit“ reicht aus, um Missbrauch auszuschließen und die Vorgaben der DS-GVO zu wahren. Recruiting und Personalentwicklung sollten explizit von der Regelung erfasst sein, um eine effiziente konzernweite Personalsteuerung zu ermöglichen. Statt pauschaler Einschränkungen sollte die Offenlegung von Beschäftigtendaten innerhalb des Konzerns für berechtigte Zwecke erlaubt sein, sofern sie erforderlich ist und datenschutzrechtliche Schutzmaßnahmen berücksichtigt werden.

   Diese Anpassungen stellen sicher, dass die Regelung praxisgerecht ist, ohne den Datenschutz der Beschäftigten zu gefährden. Gleichzeitig wird die Wettbewerbsfähigkeit und Effizienz moderner Konzernorganisationen gewahrt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Adél Holdampf-Wendel | Bereichsleiterin Future of Work & Arbeitsrecht
T 030 27576-202 | a.holdampf@bitkom.org

Isabelle Stroot | Referentin Datenschutz
T 030 27576-228 | i.stroot@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz
AK Future of Work
AK Personal & Arbeitsrecht