



Stellungnahme der GDD zu den „Vorschlägen für einen modernen Beschäftigtendatenschutz“ von BMAS und BMI

I. Einleitung und grundsätzliche Bewertung der geplanten Neuregelungen

Die zunehmende Digitalisierung stellt Arbeitgeber im Umgang mit Beschäftigtendaten vor Herausforderungen. In einem Eckpunktepapier haben das Bundesministerium für Arbeit und Soziales (BMAS) sowie das Bundesministerium des Innern und für Heimat (BMI) deshalb Eckpunkte für einen modernen Beschäftigtendatenschutz zusammengestellt. Ein Entwurf im Hinblick auf konkrete gesetzliche Regelungen soll folgen.

Die verfolgte Zielsetzung einer Konkretisierung und Anpassung der Regelungen des Beschäftigtendatenschutzes im Hinblick auf die Herausforderungen der fortschreitenden Digitalisierung der Arbeitswelt ist aus Sicht der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn, grundsätzlich positiv zu bewerten. Die geplanten Regelungen sollten sich nach Auffassung der GDD an der höchst-richterlichen Rechtsprechung orientieren, die bisher einen interessengerechten Ausgleich im Beschäftigtendatenschutz geschaffen hat. Neue Regelungen zum Beschäftigtendatenschutz sollten nicht zu einer Einschränkung der in der Rechtsprechung aufgestellten Grundsätze und Rahmenbedingungen für Unternehmen führen.

II. Europarechtliche Vorgaben

Neuregelungen zum Beschäftigtendatenschutz können nur im Rahmen des europarechtlichen Zulässigen erfolgen. Zwar sind Konkretisierungen der aktuellen Regelungen zum Beschäftigtendatenschutz wünschenswert, allerdings wäre es im Hinblick auf die verfolgte Intention des Gesetzgebers kontraproduktiv, wenn Regelungen geschaffen würden, deren Vereinbarkeit mit den Vorgaben bzw. Regelungsspielräumen der DS-GVO zweifelhaft ist. Denn auf diese Weise entstünde neue Rechtsunsicherheit. Bedeutung erlangt in diesem Zusammenhang insbes. die Reichweite der Öffnungsklausel in Art. 88 DS-GVO.



Zu berücksichtigen sind zudem die Vorgaben, die der Europäische Gerichtshof (EuGH) in seinem Urteil vom 30.3.2023 in der Rechtssache C-34/21 aufgestellt hat. Danach ergebe sich aus dem Wortlaut von Art. 88 DS-GVO, dass dessen Abs. 2 dem Ermessen der Mitgliedstaaten, die den Erlass „spezifischerer Vorschriften“ nach Abs. 1 dieses Artikels beabsichtigen, einen Rahmen setzt. So dürften sich diese Vorschriften zum einen nicht auf eine Wiederholung der Bestimmungen der DS-GVO beschränken, sondern müssten auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen (Rn. 65 der Entscheidung). Zum anderen sei dabei insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz vorzugehen (Rn. 66).

Angesichts der Vergleichbarkeit der Regelung in § 23 Abs. 1 S. 1 HDSIG zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses mit der Bestimmung in § 26 Abs. 1 S. 1 BDSG ist es naheliegend, dass auch die Bestimmung im BDSG wegen Verstoß gegen das europarechtliche Wiederholungsverbot unwirksam sein könnte.

Dies stellt den nationalen Gesetzgeber vor die Herausforderung, eine aus Sicht der Rechtsanwender verständliche und übersichtliche Regelung des Beschäftigtendatenschutzes zu schaffen, die zugleich die Vorgaben des Wiederholungsverbotes i.S. der EuGH-Entscheidung wahrt.

III. Zu den geplanten Regelungskomplexen im Einzelnen

1. Ausdehnung des Beschäftigtenbegriffs

Nach dem Eckpunktepapier sollen solselbstständige Plattformtätige in den Anwendungsbereich des Beschäftigtendatenschutzes einbezogen werden. Soloselbstständige Plattformtätige seien aufgrund der besonderen Strukturen und Geschäftsmodelle in der Plattformökonomie auch im Hinblick auf die Verarbeitung ihrer Daten vielfach in einer den Arbeitnehmerinnen und Arbeitnehmern vergleichbaren Weise schutzbedürftig.

Selbst wenn dies zutreffen sollte, scheint die geplante Ausweitung europarechtlich zweifelhaft. Soloselbstständige Plattformtätige sind nicht als „Beschäftigte“ i. S. des Art. 88 DS-GVO anzusehen. Zwar sollen vom Beschäftigtenbegriff der DS-GVO auch arbeitnehmerähnliche Personen umfasst sein, unter



Zugrundelegung der Rechtsprechung des Bundesarbeitsgerichts (BAG) sind Soloselbstständige jedoch trotz der partiell bestehenden Abhängigkeit als Selbstständige zu betrachten.

2. Keine pauschale Einschränkung von Überwachungs- und Kontrollmöglichkeiten des Arbeitgebers

Es entspricht ständiger BAG-Rechtsprechung sowie der herrschenden Literatur, dass bei der Überwachung von Beschäftigten dem berechtigten Interesse des Arbeitgebers an der Aufsicht über den Betrieb und der effektiven Organisation von Arbeitsabläufen sowie der Einhaltung gesetzlich von Arbeitgebern zu erfüllender Pflichten klare Grenzen in Gestalt des angemessenen und effektiven Schutzes des Persönlichkeitsrechts der Beschäftigten gesetzt sind. Im Sinne der Wahrung der Persönlichkeitsrechte der betroffenen Beschäftigten ist insbesondere der Grundsatz allgemein anerkannt, dass „Vollkontrollen“ von Beschäftigten nach Möglichkeit zu vermeiden und notwendige Kontrollen im Regelfall auf Stichproben zu beschränken sind. So ist die Zulässigkeit punktueller Datenerhebungen in Echtzeit, z.B. zur Erfassung von Lenk- und Ruhezeiten sowie zur Koordinierung wechselnder Arbeitseinsätze an verschiedenen Orten und der Disposition von Einsatzkräften, notwendige und sinnvolle Praxis und nach Durchführung einer entsprechenden Interessenabwägung grundsätzlich nicht zu beanstanden. Eine gesetzliche Einschränkung bestehender Überwachungs- bzw. Kontrollmöglichkeiten liefe Gefahr, den bestehenden angemessenen Ausgleich zwischen den Persönlichkeitsrechten der Beschäftigten einerseits und – ebenfalls grundrechtlich geschützten (Art. 12 und 14 GG) – Arbeitgeberpositionen andererseits unnötig zu gefährden. Sinnvoll könnte demgegenüber eine gesetzliche Regelung sein, welche die aktuell geltenden Abwägungsfaktoren bei der Beurteilung von Überwachungsmaßnahmen festhält und auf diese Weise Orientierung schafft. Verdeckte Maßnahmen des Arbeitgebers sollten dabei nicht per se ausgeschlossen werden, aber nur als „ultima ratio“ beim Verdacht schwerwiegender Verfehlungen möglich sein.

Überwachungsmaßnahmen sollten auch dann zulässig sein, wenn der konkrete Verdacht einer schwerwiegenden Verletzung arbeitsvertraglicher Pflichten zulasten des Arbeitgebers im Raum steht. Eine etwaige Beschränkung auf den Verdacht einer Straftat seitens des Beschäftigten würde die grundrechtlichen geschützten Positionen des Arbeitgebers über Gebühr einschränken. Es ist diesem nicht zuzumuten, schwerwiegende Verfehlungen der Beschäftigten nicht aufdecken und nachweisen zu können. Sofern der Verdacht von Straftaten, Ordnungswidrigkeiten oder schwerwiegenden vertraglichen Verfehlungen besteht, sollte der Arbeitgeber datenschutzrechtlich auch Maßnahmen gegen eine



identifizierte begrenzte Personengruppe ergreifen können, denn bei Einleitung interner Ermittlungsmaßnahmen kann in der Praxis ein bestehender Verdacht oftmals noch nicht auf eine konkrete Einzelperson bezogen werden.

Zur effizienten Einhaltung von Gesetzen wie internen Vorgaben (Compliance) kann es arbeitgeberseitig erforderlich sein, auch präventive Kontrollen vorzunehmen, d.h. Kontrollen ohne einen bestehenden Anhaltspunkt für das Vorliegen von Verstößen, und in diesem Zusammenhang auch personenbezogene Daten zu verarbeiten. Maßstab für die Verhältnismäßigkeit solcher präventiver Kontrollen sind u.a. deren Transparenz und das Bestehen eindeutiger Bedingungen, der Vorrang – soweit möglich – nicht-personenbezogener Datenverarbeitung sowie die Gewährleistung von Rückzugsorten und -zeiten ohne Beobachtung für die Beschäftigten.

3. Einsatz von Künstlicher Intelligenz (KI)

Zur effizienten Organisation bestimmter Arbeitsprozesse kommt es immer häufiger zum Einsatz von KI-Lösungen durch Arbeitgeber. Hinsichtlich des Einsatzes KI-gesteuerter Auswahlprozesse bedarf es Regelungen zur Erreichung umfangreicher Transparenz für die Beschäftigten, durch welche die datenschutzrechtlichen Risiken für diese minimiert werden, aber zugleich die Vorteile von KI für Wirtschaft und Beschäftigte nutzbar bleiben. Soweit einschlägig, sind die Vorgaben des Art. 22 DS-GVO zu berücksichtigen. Im Übrigen kommt der geplanten EU-KI-Verordnung besondere Bedeutung zu.

4. Datenschutz im Bewerbungsverfahren

Ob sich ein/e Bewerber/-in für das jeweilige Unternehmen eignet, gilt es für den potenziellen Arbeitgeber anhand gezielter Fragen herauszufinden. Zulässig im Rahmen des Bewerbungsverfahrens sind arbeitsplatzbezogene Fragen, die nicht an Diskriminierungsmerkmale anknüpfen und bei denen das Interesse des Arbeitgebers an einer Beantwortung das Interesse des Arbeitnehmers an einer Geheimhaltung überwiegt. Entscheidend ist jeweils das konkrete Tätigkeitsprofil der im Einzelfall zu besetzenden Stelle. Der Rahmen des Arbeitgeberfragerechts ist also recht klar durch die Rechtsprechung konturiert.

Aus Sicht der GDD kann eine gesetzliche Niederlegung der Anforderungen an das Fragerecht und konkret zulässiger bzw. unzulässiger Fragen jedoch ggf. die Anwendung der rechtlichen Vorgaben durch die Praxis erleichtern. Dabei sollte einerseits der bis dato bestehende Rahmen zulässiger Fragen nicht



eingeschränkt werden, andererseits deutlich werden, dass das Fragerecht regelmäßig nur im Einzelfall unter Berücksichtigung der konkreten Stellenbeschreibung beurteilt werden kann.

Hilfreich für die Praxis wäre eine gesetzliche Regelung der Frage, inwieweit Internetrecherchen über Bewerber/-innen zulässig sind. Während die Recherche bei Jobportalen allgemein als zulässig bewertet wird, werfen insbesondere das „Googeln“ von Kandidaten und der Umgang mit „Zufallsfunden“ praxisrelevante Fragen auf. Hier muss ein angemessener Ausgleich zwischen der Öffentlichkeit der Informationen einerseits und dem Persönlichkeitsrecht des Betroffenen andererseits gefunden werden.

Weiterhin sollte der Gesetzgeber vor dem Hintergrund des Art. 10 DS-GVO klarstellen, dass ein Fragerecht auch hinsichtlich einschlägiger Vorstrafen, die noch im Bundeszentralregister gespeichert sind, besteht. Dieses wird bereits in der Gesetzesbegründung zu § 26 BDSG unterstellt, bedarf aber der normativen Klarstellung.

5. Rechtssicherheit beim Schutz besonders sensibler Daten

Die Verarbeitung besonders sensibler Daten ist nach Art. 9 Abs. 2 DS-GVO nur in den katalogisierten Ausnahmefällen zulässig. Praktische Bedeutung hat insbesondere die Umsetzung hinsichtlich der arbeitgeber- und arbeitnehmerseitigen Rechte und Pflichten in § 26 Abs. 3 BDSG..

Im Zusammenhang mit § 26 Abs. 3 S. 1 BDSG ist umstritten, ob eine Datenverarbeitung ausschließlich zur Ausübung bzw. Erfüllung gesetzlicher Rechte und Pflichten gestattet sein soll oder ob die Verarbeitung besonderer Kategorien personenbezogener Daten legitimierende Rechte und Pflichten auch aus dem Arbeitsvertrag bzw. der arbeitsrechtlichen Beziehung erwachsen können. Für das Erfordernis einer Rechtsvorschrift spricht sich u.a. die Datenschutzkonferenz in ihrem Kurzpapier Nr. 17 „Besondere Kategorien personenbezogener Daten“ (Stand: 27.03.2018) aus. Ein solches Verständnis führt allerdings zu erheblichen Schwierigkeiten in der Praxis. So wäre etwa in Fällen, in denen das Fragerecht des Arbeitgebers auch besondere Kategorien personenbezogener Daten umfasst, die mit der Ausübung des Fragerechts verbundene Datenverarbeitung unzulässig. So ist es dem Arbeitgeber z.B. arbeitsrechtlich erlaubt, im Bewerbungsgespräch nach Krankheiten zu fragen, die zur dauerhaft fehlenden Eignung des Bewerbers führen. Im Rahmen von § 26 Abs. 3 S. 1 BDSG sollte insofern ein Gleichlauf mit dem Fragerecht des Arbeitgebers hergestellt werden.



6. Interessenabwägung handhabbarer machen

Die Aufführung typischerweise relevanter Kriterien für die Durchführung der Interessenabwägung kann aus Sicht der GDD die praktische Anwendung der Vorschriften zum Beschäftigtendatenschutz erleichtern und daher sinnvoll sein, sofern sichergestellt ist, dass keine pauschalen Aussagen über die Zulässigkeit der Datenverarbeitung entstehen, sondern die Interessenabwägung weiterhin einzelfallbezogen unter Berücksichtigung aller jeweiligen Detailumstände erfolgt.

7. Freiwilligkeit der Einwilligung

Aufgrund der strukturellen Unterlegenheit des Arbeitnehmers bzw. der Arbeitnehmerin gegenüber dem Arbeitgeber ist die Freiwilligkeit der Einwilligung eines bzw. einer solchen in jedem Fall besonders zu prüfen (vgl. § 26 Abs. 2 S. 1 und 2 BDSG). Der Einwilligung von Beschäftigten kommt im Kontext des Datenschutzes hohe Bedeutung zu. Die Freiwilligkeit ist zu bejahen, wenn der/die Beschäftigte die Einwilligung ohne Befürchtung von Sanktionen verweigern darf. Hierzu bedarf es aus Sicht der GDD keiner zusätzlichen Konkretisierung.

Zu beachten ist, dass nicht nur Einwilligungen von Beschäftigten in die Veröffentlichung ihrer Fotos im Intranet freiwillig sein können, sondern auch entspr. Einwilligungen in die Veröffentlichung im Internet. Auch Letztere können ohne Druck abgegeben sein. Entscheidend ist stets der Einzelfall.

8. Mehr Rechtssicherheit bei Konzerndatenverarbeitung

Für die Zulässigkeit konzerninterner Datenübermittlungen, z.B. zentralisierte Verwaltungsorganisationen oder die Arbeit in Matrixstrukturen ist durch konkrete Regelungen für praxisrelevante Fallgruppen Rechtssicherheit zu schaffen. Dadurch können bürokratische Hürden gesenkt und die Flexibilität gefördert werden.

9. Betroffenenrechte

Die DS-GVO sieht umfassende Rechte für betroffene Personen zu, wozu auch Beschäftigte zählen. Bereits jetzt stellt die Geltendmachung von Betroffenenrechten die Verantwortlichen aufgrund der ohnehin bestehenden Reichweite der Rechte vor immense, praktisch handhabbare Herausforderungen. Das gilt insbesondere für die Geltendmachung des Auskunftsrechts (Art. 15 DS-GVO) durch ehemalige Arbeitnehmer/-innen, die das Recht aus datenschutzfremden Motiven ausüben. Die hieraus



resultierende Konfliktlage und Belastung der Wirtschaft sollten nicht noch durch eine Ausweitung der Rechte verschärft werden.

10. Beweisverwertung

Aus einer unzulässigen Datenverarbeitung darf nicht zwangsläufig ein prozessuales Beweisverwertungsverbot folgen. Die Annahme eines Verwertungsverbotes bedarf stets einer Interessenabwägung. Ein Verwertungsverbot beispielsweise heimlicher Videoaufzeichnungen wegen der Verletzung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ergibt sich nur, wenn die Aufzeichnung nicht im Einzelfall durch überwiegende Interessen an der Wahrheitsfindung gerechtfertigt ist. Die Normierung eines generellen Verwertungsverbotes bei Datenschutzverstößen liefe zudem dem Prinzip der freien richterlichen Beweiswürdigung zuwider.

11. Betriebliche Nutzung privater Endgeräte (BYOD)

Für den Fall, dass Arbeitnehmer ihre privaten Endgeräte für betriebliche Zwecke (z.B. im Home-Office) nutzen, müssen Anforderungen des Beschäftigtendatenschutzes konkretisiert werden und Rechtsklarheit für die Praxis geschaffen werden. Insbesondere ist darauf zu achten, dass die Nutzung der privaten Endgeräte nicht zu einem Unterlaufen der Voraussetzungen des Art. 32 DS-GVO führt. An den privaten Endgeräten müssen entsprechende Schutzvorkehrungen getroffen werden, um der Datensicherheit Rechnung zu tragen.

12. Mitbestimmung des Betriebsrats

Entsprechend der Verabredung im Koalitionsvertrag soll die Mitbestimmung durch Betriebs- und Personalräte weiterentwickelt werden. Neuregelungen und Anpassungen sind aus Sicht der GDD nur insoweit erforderlich, wie digitale Prozesse beschleunigt werden können. Denn Mitwirkungsrechte des Betriebsrates beim Einsatz von KI sind bereits jetzt geregelt: Hinsichtlich der Implementierung von KI-Systemen können sich Beteiligungsrechte des Betriebsrats bereits heute aus § 90 Abs. 1 Nr. 2 oder Nr. 3 BetrVG ergeben.



13. Kollektivrechtliche Regelungen

Wie das BMAS und BMI sieht auch die GDD Betriebsvereinbarungen als betriebsnahes und praxisgerechtes Instrument zur Konkretisierung des Beschäftigtendatenschutzrechts im Hinblick auf spezifische Verarbeitungskonstellationen in der Praxis. Betriebsvereinbarungen ermöglichen es, klare und für die Beschäftigten transparente Datenschutzregelungen speziell für einen Betrieb herauszuarbeiten.

Praxisrelevant im Zusammenhang mit kollektivrechtlichen Regelungen ist v.a. die umstrittene Frage, inwiefern die Betriebsparteien auf denen ihnen eröffneten Regelungsgebieten nicht nur eine Konkretisierung, sondern auch Verbesserung bzw. Verschlechterung des von der DS-GVO begründeten Persönlichkeitsrechtsschutzes herbeiführen können. Sinnvoll wäre diesbezüglich eine gesetzliche Klarstellung, dass nicht jedes partielle Abweichen nach unten vom Schutzstandard der DS-GVO unzulässig ist, sondern es vielmehr einer Gesamtbetrachtung der innerbetrieblichen Regelung bedarf und insbes. zu prüfen ist, ob die von Art. 88 Abs. 2 DS-GVO geforderten Maßnahmen zum Schutz der Beschäftigten eingehalten sind.

Bonn, den 17.05.2023

Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen - insbesondere auch die Datenschutzbeauftragten - bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen Anforderungen zu unterstützen.

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de | www.gdd.de