Juni 2024

Stärkung der Datenschutz-rechte von Arbeitnehmer*innen

Wie Gewerkschaften und Betriebsräte mithilfe von Kollektivverhandlungen Datenschutzstandards am Arbeitsplatz festhalten können

Halefom Abraha

Arbeitnehmer*innenrechte im digitalen Zeitalter

FRIEDRICH EBERT STIFTUNG

ARBEITNEHMER*INNENRECHTE IM DIGITALEN ZEITALTER

STÄRKUNG DER DATENSCHUTZRECHTE VON ARBEIT-NEHMER*INNEN

Wie Gewerkschaften und Betriebsräte mithilfe von Kollektivverhandlungen Datenschutzstandards am Arbeitsplatz festhalten können

Inhalt

ZUSAMMENFASSUNG

Die Einhaltung geltender Datenschutzgesetze am Arbeitsplatz gilt als mangelhaft. Dafür gibt es verschiedene Gründe, unter anderem die rechtliche Unklarheit. Um die Einhaltung der Datenschutzbestimmungen am Arbeitsplatz zu verbessern, müssen folglich die Standards der Datenschutz-Grundverordnung (DSGVO) für die Arbeitsumgebung spezifiziert werden.

In dieser Abhandlung geht es in erster Linie um Art. 88 DSGVO, der den EU-Mitgliedstaaten die Möglichkeit einräumt, »spezifischere Vorschriften [...] hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext« vorzusehen. Dies kann in Form von nationalen Gesetzen oder Kollektivvereinbarungen einschließlich sogenannter »Betriebsvereinbarungen« (also Vereinbarungen auf Firmenebene) erfolgen. Hierin wird dargelegt, an welcher Stelle die DSGVO für den Beschäftigungskontext präzisiert werden muss und wie Gewerkschaften und Betriebsräte dieses Thema angehen können. Diese Abhandlung richtet sich vorrangig an Gewerkschaften und Betriebsräte, die Vereinbarungen zum Datenschutz aushandeln, kann aber auch Impulse für nationale Gesetze zum Datenschutz am Arbeitsplatz geben.

Sie legt verschiedene Datenschutzaspekte dar, darunter die Aufgaben der Gewerkschaften und Betriebsräte:

- **Klärung inhaltlicher und formeller Anforderungen** einschließlich der Bedingungen für die Einwilligung als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten von Arbeitnehmer*innen, die Auflagen bei der Verwendung von Technologien wie Emotionserkennung und wie Arbeitnehmer*innen in Datenschutz-Folgenabschätzungen einbezogen werden sollten.

- **Festlegung des Umfangs der individuellen und kollektiven Datenrechte** durch Schaffung von Rahmenbedingungen, damit Arbeitnehmer*innen ihre Rechte auf Information über und Zugriff auf ihre personenbezogenen Daten wirksam ausüben können, und durch Aushandlung zusätzlicher kollektiver Rechte auf Datenzugriff, Information und Streitbeilegung, die über die DSGVO hinausgehen.

- **Festlegung klarer Vorgaben für algorithmisches Management**, zum Beispiel hinsichtlich der Gestaltung, Bereitstellung und Nutzung algorithmischer Systeme, des nötigen Transparenzgrades (hoch!) und der Möglichkeit für Gewerkschaften und Betriebsräte, das Recht auf Überprüfung von Algorithmen einzufordern und in Entscheidungen im Laufe des Technologie-Lebenszyklus einbezogen zu werden.

Die hiermit einhergehende Publikation »Besserer Datenschutz am Arbeitsplatz« erörtert diverse weitere, noch nicht ausgereizte Möglichkeiten im Rahmen der DSGVO, Standards für den Datenschutz am Arbeitsplatz zu formulieren, zum Beispiel durch Festlegung von Verhaltensregeln und Zertifizierungssystemen gemäß den Artikeln 40 und 42 DSGVO.

EINLEITUNG

Arbeitnehmer*innen haben spezielle Datenschutzbedürfnisse, die von allgemeinen Datenschutzvorschriften möglicherweise nicht vollständig erfüllt werden. Darum räumt Art. 88 DSGVO den Mitgliedstaaten und Sozialpartnern die Möglichkeit ein, ausführlichere Vorschriften für den Beschäftigungskontext zu erlassen. Derzeit herrscht angesichts der Untätigkeit der Mitgliedstaaten bei der Anwendung von Artikel 88 eine gewisse Rechtsunsicherheit. Die Sozialpartner sollten trotzdem nicht darauf warten, dass die Mitgliedstaaten aktiv werden. Art. 88 DSGVO ermöglicht es den Sozialpartnern, die Datenrechte von Arbeitnehmer*innen durch Festlegung konkreterer Standards in Kollektivverhandlungen zu schützen.

Mit der zunehmenden Digitalisierung der Arbeitsumgebung steigt auch der Bedarf an soliden Kollektivvereinbarungen. Die Sozialpartner sind bestens aufgestellt, um die Datenschutzrisiken für Arbeitnehmer*innen zu ermitteln, den Ursprung, Schweregrad, die Art und Wahrscheinlichkeit dieser Risiken einzuschätzen, spezielle Schutzmaßnahmen festzulegen und die ordnungsgemäße Anwendung bestehender Vorschriften zu überwachen. Daher geht es in dieser Abhandlung um die konkreten Datenschutzbereiche, auf deren Klärung sich Gewerkschaften und Betriebsräte bei ihren Vereinbarungen mit den Arbeitgebern konzentrieren sollten.

Die für die Arbeitnehmer*innen günstigeren gesetzlichen Vorschriften der Mitgliedstaaten und allgemeinen Anforderungen und Grundsätze der DSGVO haben in jedem Fall Vorrang vor den detaillierten Vorgaben, die von den Sozialpartnern für das Arbeitsumfeld eingeführt werden.

1

INHALTLICHE UND FORMALE ANFORDERUNGEN

1.1 KLÄRUNG DES EINWILLIGUNGS-VORBEHALTS

Die »Einwilligung« im Sinne der DSGVO stellt nur dann eine wirksame Rechtsgrundlage dar, wenn sie in Kenntnis der Sachlage, für den konkreten Fall, freiwillig und unmissverständlich erteilt wird. Aufsichtsbehörden, politische Entscheidungsträger*innen und Arbeitnehmervertretungen sehen dies jedoch aufgrund des inhärenten Macht- und Informationsgefälles zwischen Arbeitgeber*innen und Arbeitnehmer*innen schon seit Längerem als eine unzureichende Rechtsgrundlage für die Verarbeitung personenbezogener Beschäftigtendaten an.

Im Beschäftigungskontext kann die Einwilligung also in der Regel nicht als »freiwillig erteilt« im Sinne der DSGVO angesehen werden. Aufgrund des Machtgefälles haben Arbeitnehmer*innen vermutlich auch nicht wirklich die Möglichkeit, ihre Einwilligung zu verweigern, ohne Konsequenzen fürchten zu müssen. Darüber hinaus schmälert die Nutzung intransparenter und ausgeklügelter Überwachungs- und algorithmischer Managementsysteme die Gültigkeit der Einwilligung zusätzlich: Die Arbeitnehmer*innen wissen gar nicht, wie diese Technologien funktionieren, in welchem Umfang und mit welchen Folgen Daten erhoben werden und worin sie einwilligen, wodurch der Grundsatz der »Einwilligung in Kenntnis der Sachlage« nicht mehr gegeben ist.

In Anerkennung dieses Problems gestattet die DSGVO, dass Kollektivvereinbarungen einschließlich Betriebsvereinbarungen konkrete Vorgaben zu den Bedingungen enthalten, unter denen personenbezogene Daten im Beschäftigungskontext auf Grundlage der Einwilligung verarbeitet werden dürfen (Erwägungsgrund 155). Dadurch bietet sich den Gewerkschaften und Betriebsräten eine Gelegenheit, mit den Arbeitgeber*innen zu verhandeln. Gewerkschaften und Betriebsräte sollten zumindest:

i. Die Arbeitgeber*innen auffordern, eine andere Rechtsgrundlage als die Einwilligung zur Verarbeitung der Beschäftigtendaten heranzuziehen. Geeignete Rechtsgrundlagen sind unter anderem die Notwendigkeit zur Erfüllung des Arbeitsvertrags (Art. 6 Abs. 1 Bst. b); zur Erfüllung einer externen rechtlichen Verpflichtung (Art. 6 Abs. 1 Bst. c); oder zum Schutz lebenswichtiger Interessen der Arbeitskraft oder einer anderen natürlichen Person (Art. 6 Abs. 1 Bst. d). Die anderen Rechtsgrundlagen – Notwendigkeit im öffentlichen Interesse (Art. 6 Abs. 1 Bst. e) und aus berechtigtem Interesse des Arbeitgebers / der Arbeitgeberin (Art. 6 Abs. 1 Bst. f) – sind rechtlich mehrdeutig und sollten daher vermieden werden.

ii. Genau darlegen, unter welchen Bedingungen die Einwilligung als Rechtsgrundlage dienen darf, zum Beispiel, wenn dadurch ein deutlicher rechtlicher oder wirtschaftlicher Vorteil für die Arbeitskraft entsteht. Gewerkschaften und Betriebsräte sollten aber auch Zusammenhänge, Zwecke, Vorgehensweisen und Verarbeitungstätigkeiten bestimmen, bei denen eine Einwilligung unzulässig ist, zum Beispiel zur Bereitstellung algorithmischer Managementsysteme.

iii. Dafür sorgen, dass leicht zugängliche Rücktrittsoptionen ausgehandelt werden, mit denen die Arbeitnehmer*innen ihre Einwilligung ohne Angst vor nachteiligen Konsequenzen widerrufen können, wenn die Einwilligung als Rechtsgrundlage verwendet wird.

1.2 EINSCHRÄNKUNG BESTIMMTER TECHNOLOGIEN, VERFAHREN UND ZWECKE

Bestimmte Datenverarbeitungsvorgänge im Beschäftigungskontext bergen ein erhebliches Risiko für die Menschenwürde sowie für die berechtigten Interessen und Grundrechte der Arbeitnehmer*innen. Das trifft vor allem dann zu, wenn die Verarbeitung weit über das hinausgeht, was für ein klar definiertes berechtigtes Interesse nötig und angemessen ist; wenn die Verarbeitung über das hinausgeht, was zur Erfüllung eines Arbeitsvertrags nötig ist; oder wenn die Verarbeitung die vorhandenen Kontrollstufen, die Eigenständigkeit und das Vertrauen beeinträchtigt.

Gewerkschaften und Betriebsräte sollten eindeutige Verbote für potenziell schädliche Überwachungstechnologien wie Emotionserkennung sowie schädliche Praktiken und Zwecke wie psychische oder emotionale Manipulation verhängen.[1]

1 Hinweis: In der EU-Richtlinie zur Plattformarbeit, die am 24. April 2024 vom Europäischen Parlament erlassen wurde und noch vom Europarat genehmigt und im Amtsblatt der EU veröffentlicht wer-

Gewerkschaften und Betriebsräte spielen eine entscheidende Rolle bei der Festlegung der konkreten Bedingungen, unter denen eine Überwachung von Arbeitskräften annehmbar ist. Dabei sollten in erster Linie klare Grenzen für die Überwachung, vor allem außerhalb der Arbeitszeit – zum Beispiel während der Pausen oder Ruhezeiten – festgelegt werden. Angesichts der zunehmend verschwimmenden Grenzen zwischen Berufs- und Privatleben ist dies unumgänglich. Ein wesentlicher Aspekt bei diesen Verhandlungen ist das Verbot von Überwachungspraktiken, die die Privatsphäre der Arbeitnehmer*innen verletzen. Dazu gehört auch die Überwachung der privaten Kommunikation von Arbeitnehmer*innen, die nichts mit ihren wesentlichen Aufgaben zu tun hat, und ihrer Gespräche mit Gewerkschaftsvertreter*innen. Ständige Überwachung sollte verboten sein, sofern sie nicht aus Gesundheits- oder Sicherheitsgründen oder zum Schutz von Eigentum unbedingt notwendig ist.

Zudem muss unbedingt sichergestellt werden, dass sich die Überwachung nicht auf die Beobachtung des Verhaltens von Arbeitskräften erstreckt mit dem Ziel, sie an der Ausübung ihrer gesetzlichen Rechte zu hindern, darin einzugreifen, sie dazu zu zwingen oder entsprechende Vorhersagen, Feststellungen oder Darstellungen vorzunehmen. Diese Rechte betreffen insbesondere das Recht auf Vereinigungsfreiheit und Teilnahme an Kollektivverhandlungen durch von den Beschäftigten selbst gewählte Vertreter*innen. Zum Schutz der Würde und zur Wahrung der Rechte der Arbeitskräfte und Aufrechterhaltung einer fairen und respektvollen Arbeitsumgebung ist es nötig, solche Überwachungspraktiken zu verbieten.

1.3 ABWÄGUNG DER INTERESSEN VON ARBEITNEHMER*INNEN UND ARBEITGEBER*INNEN

Das Schwierigste an der Datenverarbeitung im Beschäftigungskontext ist die Herbeiführung eines ausgewogenen Verhältnisses zwischen den berechtigten Interessen der Arbeitgeber*innen und den Rechten der Arbeitnehmer*innen auf Würde, Privatsphäre und anderen Grundrechten. Die Frage der Verhältnismäßigkeit stellt sich vor allem dann, wenn die Verarbeitung von Beschäftigtendaten über das hinausgeht, was im Rahmen des vertraglich geregelten Beschäftigungsverhältnisses unbedingt notwendig ist. Jede Verarbeitung von Beschäftigtendaten, die nicht in direktem Zusammenhang mit der Erfüllung des Arbeitsvertrags steht und nicht zwingend dafür notwendig ist, darf erst nach einer sorgfältigen Abwägung der Interessen erfolgen. Dazu gehört auch, die »berechtigten Interessen« von Arbeitgeber*innen – die oftmals als vorrangige Rechtsgrundlage für die Einführung automatisierter Überwachungs- und Entscheidungstechnologien am Arbeitsplatz angeführt werden – zu bewerten.

Leider beinhalten die derzeitigen Gesetze keine eindeutigen Vorgaben, wie solche Abwägungen durchzuführen sind. Was genau als berechtigtes Interesse gilt, ist nach wie vor unklar, kontextabhängig und anfällig für Missbrauch. Die Auffassung ändert sich mit der Zeit, den Umständen und Geschäftsmodellen. Arbeitgeber*innen können ganz einfach argumentieren, dass jede Form von Überwachung und Kontrolle am Arbeitsplatz angemessen und für die Interessen des Unternehmens und die Zwecke, die sie selbst festlegen, nötig ist, um zum Beispiel die Produktivität, Effizienz und den Fortschritt zu fördern.

So entschied 2023 das Verwaltungsgericht Hannover entgegen der Auffassung der Landesdatenschutzbeauftragten, dass die durchgängige elektronische Überwachung der Aktivitäten einzelner Arbeitskräfte gesetzlich zulässig war, da der Arbeitgeber ein berechtigtes Geschäftsinteresse an der Erhebung und Verarbeitung dieser Daten hatte – zum einen für Organisation der Arbeit in Echtzeit und zum anderen für Personalentscheidungen bezüglich Schulungen, Feedback und Leistungsbewertungen (siehe auch Abraha 2023). Die Landesdatenschutzbeauftragte von Niedersachsen ist nach wie vor der Ansicht, dass ihre ursprüngliche Einschätzung korrekt ist, und hat 2023 gegen das Urteil Berufung eingelegt. Zwar würden die meisten Datenschutzexpert*innen in diesem Fall vermutlich der Landesdatenschutzbeauftragten zustimmen, aber gleichzeitig ist zu erwähnen, dass die DSGVO selbst wichtige Begriffe wie »berechtige Interessen« weder eindeutig definiert noch vorgibt, wie solche Interessen – selbst wenn sie »berechtigt« sind – gegen die Rechte der betroffenen Personen und ihr Interesse am Schutz ihrer personenbezogenen Daten abzuwägen sind, einschließlich der grundlegenden Datenschutzprinzipien wie der Datenminimierung.

Gewerkschaften und Betriebsräte sollten daher den aktiven Dialog mit den Arbeitgeber*innen suchen und Verhandlungen führen, um klare Rahmenbedingungen für eine gerechte Abwägung der Interessen von Arbeitnehmer*innen und Arbeitgeber*innen zu schaffen. Dazu gehört auch ein transparentes, einvernehmliches Verständnis dessen, was ein »berechtigtes Interesse« darstellt und wie es in Einklang mit den Datenrechten der Beschäftigten gebracht werden kann.

Gewerkschaften und Betriebsräte sind in der idealen Position, individuelle Lösungen anzubieten, die den spezifischen Bedürfnissen der verschiedenen Arbeitsplätze oder Sektoren entsprechen. Diese Vorgaben können über die in der DSGVO geforderten Mindeststandards hinausgehen und bei Bedarf besseren Schutz bieten. Sie können die Zusammenhänge, Zwecke, Praktiken und Verarbeitungsaktivitäten, die tabu sein sollten – zum Beispiel die kontinuierliche Überwachung der Beschäftigten – darlegen. Außerdem können sie festhalten, unter welchen Umständen und bei welchen Verarbeitungstätigkeiten »berechtigte Interessen« nicht als valide Rechtsgrundlage angeführt werden können.

---

den muss, wird die Verarbeitung *jeglicher* personenbezogener Daten über den emotionalen oder psychischen Zustand von Plattformbeschäftigten; jeglicher personenbezogener Daten in Bezug auf private Unterhaltungen, insbesondere mit Arbeitnehmervertretungen; und die Erhebung jeglicher personenbezogener Daten von Arbeitskräften außerhalb der Arbeitszeit durch digitale Arbeitsplattformen verboten (Art. 7 Abs. 1 Bst. a-c). Siehe auch Adams-Prassl et al. 2023 (Regulating algorithmic management: a blueprint, *European Labour Law Journal*, 2023), S. 128-131.

1.4 KLÄRUNG DER FRAGE, WIE SICH ARBEITGEBER/IN UND BETRIEBSRAT GEGENSEITIG BEI DER EINHALTUNG DER DATENSCHUTZPFLICHTEN UNTERSTÜTZEN SOLLTEN

Arbeitnehmervertretungen wie Gewerkschaften und Betriebsräte verarbeiten personenbezogene Daten von Arbeitnehmer*innen, die unter Umständen gemäß Art. 9 DSGVO auch vertraulich sein können. Gewerkschaften sind unabhängige Rechtspersonen. Ihre Verarbeitung personenbezogener Beschäftigtendaten wird daher normalerweise gemäß DSGVO geregelt. Gewerkschaften sind also »normale« Datenverantwortliche und müssen die gleichen Pflichten wie alle anderen Datenverantwortlichen auch erfüllen.

Bei Betriebsräten ist die rechtliche Situation allerdings etwas komplizierter: Sie sind in der Regel keine unabhängige Rechtsperson, sondern gehören zur Arbeitgeberorganisation. Betriebsräte haben aber mitunter Zugang zu personenbezogenen Beschäftigtendaten, auf die der/die Arbeitgeber/in nicht zugreifen kann (und sollte). Die Ziele und Interessen des Betriebsrates weichen unter Umständen von denen des Unternehmens ab. Nichtsdestotrotz gilt ein Betriebsrat im Sinne der Konformität mit den Datenschutzgesetzen scheinbar nach wie vor als »Teil« des Unternehmens.

Daraus kann eine unklare Rechtslage entstehen, die viele Fragen aufwirft. Wenn der Betriebsrat beispielsweise zur Ausübung seines Informations- und Anhörungsrechts das Unternehmen um Informationen bittet, inwiefern kann das Unternehmen sich auf seine Pflichten gemäß Datenschutzgesetz berufen, um eine solche Anfrage abzuweisen? Allgemeiner ausgedrückt: Wie handhaben Arbeitgeber*innen solche Anfragen? Wenn der Betriebsrat zum Beispiel das Unternehmen nach personenbezogenen Daten von Arbeitnehmer*innen fragt, diese Arbeitnehmer*innen aber nicht darin einwilligen, dass der Betriebsrat diese Daten erhalten oder verarbeiten darf, kann sich der Betriebsrat dann auf andere Rechtsgrundlagen wie berechtigte Interessen berufen? Ein anderes Thema: Inwiefern sind Arbeitgeber*innen verpflichtet, die technische Infrastruktur und Expertise zu finanzieren, um sicherzustellen, dass personenbezogene Daten vom Betriebsrat sicher verarbeitet werden und dass der Betriebsrat seinen Pflichten gegenüber den Arbeitnehmer*innen in Bezug auf ihre Datenschutzrechte (z. B. Recht auf Zugang, Berichtigung, …) zeitnah und zufriedenstellend nachkommen kann, obwohl die Arbeitgeber*innen selbst gar nicht auf diese Daten zugreifen dürfen?

Eine vorläufige Untersuchung »grauer Literatur« in ausgewählten Mitgliedstaaten ergab, dass der rechtliche Rahmen rund um diese Aspekte gerade erst in der Entstehung begriffen ist und noch viele Fragen offen sind. Betriebsräte und Gewerkschaften könnten derweil zumindest versuchen, in Kollektivvereinbarungen auf Werks-, Firmen- oder Sektorebene einige Fragen bezüglich der Verarbeitung personenbezogener Beschäftigtendaten zu klären, zum Beispiel:

i. Ein gemeinsames Verständnis der Datenschutzpflichten des Betriebsrates gemäß des national geltenden Arbeitsrechts.

ii. Einvernehmen darüber, dass der Betriebsrat personenbezogene Daten, auf die das Unternehmen keinen Zugriff hat (und auch nicht haben sollte), erheben, speichern und verarbeiten darf, selbst wenn er im Sinne des Datenschutzgesetzes kein unabhängiger »Datenverantwortlicher«, sondern Teil des Unternehmens ist.

iii. Einvernehmen darüber, dass es ungeachtet (ii) im Interesse der Arbeitgeber*innen liegt, die Betriebsräte zu unterstützen, insbesondere durch Zugang zur technischen Infrastruktur und Expertise, um sicherzustellen, dass der Betriebsrat über die nötigen Kapazitäten zur datenschutzrechtskonformen Verarbeitung personenbezogener Daten verfügt. Beispielsweise muss gewährleistet sein, dass Daten sicher verwahrt und, wenn sie nicht mehr benötigt werden, gelöscht werden und dass Arbeitnehmer*innen ihre Datenschutzrechte bezüglich der Verarbeitung ihrer personenbezogenen Daten durch den Betriebsrat ausüben können.

iv. Festlegung konkreter, bereitzustellender Mittel bezüglich (iii), z. B. Bereitstellung spezieller technischer Ressourcen und Mitarbeiter*innen, um sicherzustellen, dass der Betriebsrat seinen Datenschutzpflichten nachkommen kann.

1.5 EINBEZIEHUNG IN DATENSCHUTZ-FOLGENABSCHÄTZUNGEN (DSFA)

Wenn Datenverarbeitungsaktivitäten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Arbeitnehmer*innen darstellen, müssen Arbeitgeber*innen gemäß Art. 35 DSGVO vorab eine DSFA durchführen. Vor allem die Einführung neuer Technologien am Arbeitsplatz birgt ein solches Risiko. Die DSGVO legt dar, was eine DSFA beinhalten sollte. Dazu gehören unter anderem eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit, eine Bewertung der Risiken für die Rechte und Freiheiten der Arbeitnehmer*innen sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen. Die DSGVO bietet zwar keine präzise Definition für ein »hohes Risiko«, aber Art. 35 Abs. 3 enthält eine nicht erschöpfende Liste entsprechender Verarbeitungstätigkeiten wie automatisierte Entscheidungsfindung. In den europäischen DSFA-Leitlinien wird die Überwachung von Arbeitnehmer*innen ebenfalls als hohes Risiko eingestuft und ihre Schutzbedürftigkeit (Erwägungsgrund 75) vor systematischer Überwachung (Art. 35 Abs. 3 Bst. c) angeführt. Folglich klassifizieren viele Aufsichtsbehörden die »Beschäftigtenüberwachung« als Aktivität, die immer eine DSFA erfordert.

Wie wirksam eine DSFA ist, hängt jedoch erheblich davon ab, inwieweit die Arbeitnehmer*innen oder ihre Vertretung in den Vorgang einbezogen und ihre Ansichten berücksich-

tigt werden. In Deutschland ist die Einbeziehung des Betriebsrates gemäß Arbeitsgesetz vorgeschrieben, aber in anderen Mitgliedstaaten ist das nicht der Fall. Laut DSGVO Art. 35 Abs. 9 sollen die Arbeitgeber*innen »gegebenenfalls« den Standpunkt der Arbeitnehmer*innen oder ihrer Vertretung einholen – ein Ausdruck, der von den Arbeitgeber*innen selbst ausgelegt wird und unter Umständen die Arbeitnehmerbeteiligung einschränkt.

Aus diesem Grund sollten sich Gewerkschaften und Betriebsräte für eine durchgängige Beteiligung an DSFA-Vorgängen gemäß Art. 35 Abs. 9 DSGVO einsetzen. Diese Bestimmung ist eng auszulegen, damit die Einbeziehung der Arbeitnehmer*innen oder ihrer Vertretung verpflichtend wird. Gewerkschaften und Betriebsräte müssen dieses Recht geltend machen. Es sollte in der Verantwortung der Arbeitgeber*innen liegen, eine fehlende Rücksprache während einer DSFA zu rechtfertigen. Darüber hinaus sollten sie potenziell »hochriskante« Datenverarbeitungsszenarien ermitteln und für angemessene technische und organisatorische Maßnahmen zur Abschwächung dieser Risiken sorgen. Diese Verantwortung ist entscheidend, denn laut Art. 35 Abs. 1 sind »Umstände und Zweck« der Verarbeitung maßgebliche Faktoren bei der Risikobewertung. Und nicht zuletzt müssen Gewerkschaften und Betriebsräte sicherstellen, dass DSFA regelmäßig überprüft werden, vor allem, wenn neue oder andere Verarbeitungsvorgänge das Risiko beeinflussen.

2

INDIVIDUELLE UND KOLLEKTIVE DATENRECHTE

2.1 DAS INFORMATIONSRECHT AUSDRÜCKLICH FESTHALTEN

Der Transparenzgrundsatz ist eine wesentliche Voraussetzung, um die Verantwortung und Ausübung der Datenrechte von Arbeitnehmer*innen zu gewährleisten. Art. 88 Abs. 2 DSGVO sieht ausdrücklich vor, dass in Kollektivvereinbarungen festgehaltene Vorschriften insbesondere Maßnahmen im Hinblick auf die Transparenz der Verarbeitung enthalten sollten. Außerdem ist in der DSGVO festgelegt, welche Informationen den Arbeitnehmer*innen zur Verfügung stehen sollten, wie sie zu kommunizieren sind und wann solche Mitteilungen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten erfolgen sollten. Gewerkschaften und Betriebsräte können erheblich Einfluss darauf nehmen, wie das »Informationsrecht« durch Kollektivvereinbarungen unbeschadet vorteilhafterer gesetzlicher Vorschriften um- und durchgesetzt wird. In diesem Zusammenhang sollte das Informationsrecht zumindest die folgenden Aspekte behandeln:

i. **Zeitrahmen:** Arbeitnehmer*innen sollten dreimal über die Datenverarbeitungspraktiken im Rahmen ihrer Beschäftigung informiert werden: bei der Bewerbung, bei Vorlage des Arbeitsvertrags und während des Beschäftigungsverhältnisses. Die DSGVO sieht je nach Datenquelle und Verarbeitungszweck konkrete Fristen für diese Mitteilungen vor. Wenn personenbezogene Daten direkt von einer Arbeitskraft erhoben werden, muss diese zu Beginn des Verarbeitungszyklus darüber informiert werden. Wenn die Daten aus anderen Quellen stammen, muss die Person »innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats« informiert werden. Um »Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden«, müssen Arbeitnehmer*innen vor Beginn der neuen Verarbeitung informiert werden.

   Gewerkschaften und Betriebsräte sollten Leitlinien bereitstellen, wie diese Anforderungen umzusetzen sind. Außerdem sollten sie dafür sorgen, dass Arbeitnehmer*innen umfassend über alle neuen Überwachungs- und Entscheidungstechnologien informiert werden, bevor diese am Arbeitsplatz eingeführt werden.

ii. **Kategorien personenbezogener Daten und eine Beschreibung der Verarbeitungszwecke:** In der DSGVO wird in den Artikeln 13 und 14 ausführlich dargelegt, welche Informationskategorien den Arbeitnehmer*innen zur Verfügung gestellt werden müssen. Diese Vorgabe gilt unabhängig davon, ob die personenbezogenen Daten direkt von der Arbeitskraft oder von einer anderen Quelle erhoben wurden. Laut Art. 13 Abs. 2 Bst. f und Art. 14 Abs. 2 Bst. g DSGVO müssen den Arbeitnehmer*innen folgende Kategorien personenbezogener Daten zur Verfügung gestellt werden: (1) das Bestehen einer automatisierten Entscheidungsfindung; (2) aussagekräftige Informationen über die involvierte Logik; und (3) die Tragweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Arbeitskraft. Die Pflicht, über das Vorhandensein einer automatisierten Entscheidungsfindung zu informieren, ist zwar relativ eindeutig, aber die anderen Aspekte sind kontrovers und können in der Praxis für Verunsicherung sorgen (siehe Custers und Heijne, 2022). Die DSGVO legt nicht fest, was mit »aussagekräftigen Informationen über die involvierte Logik« gemeint ist. Die vorhandene Literatur legt jedoch nahe, dass diese Formulierung im Einklang mit dem zugrundeliegenden Recht auf Information und dem Transparenzgrundsatz zu deuten ist. Zu allgemeine oder zu detaillierte Informationen sind unter Umständen nicht hilfreich und erfüllen nicht das Kriterium der Aussagekraft. So ist beispielsweise eine komplizierte technische Erläuterung des algorithmischen Managementsystems ebenso wenig aussagekräftig wie ein bloßer Hinweis auf die Verwendung eines automatisierten Entscheidungsfindungssystems. Gewerkschaften und Betriebsräte können daher wesentlich dazu beitragen, diese Anforderungen im Beschäftigungskontext näher zu erläutern und auszuweiten.[2]

iii. **Die Art und Weise der Informationsübermittlung an einzelne Arbeitnehmer*innen:** Die DSGVO legt fest, dass Informationen den Arbeitnehmer*innen präzise, transparent, nachvollziehbar, leicht zugänglich und in einfacher, verständlicher Sprache zur Verfügung ge-

2 Ausführlichere Informationen, wie diese Anforderungen ausgeweitet werden können, finden sich in Adams-Prassl et al. 2023 (Regulating algorithmic management: a blueprint, European Labour Law Journal, 2023), Policy Option 3.

stellt werden müssen. Die Arbeitgeber*innen, und Datenverantwortliche im Allgemeinen, erfüllen diese Anforderungen jedoch nicht immer, wenn sie auf Zugriffsanfragen von Datensubjekten reagieren. Bei einer Studie mit Uber-Fahrer*innen stellte sich zum Beispiel heraus, dass das Unternehmen den Fahrer*innen auf ihre Bitte um Auskunft über ihre personenbezogenen Daten jeweils 26 separate »Rohdaten«-Dateien zukommen ließ (Stein et al. 2023) – ein unbrauchbarer, überwältigender Haufen aus Daten, mit denen die meisten Arbeitnehmer*innen vermutlich nichts anfangen können. Zudem sollten die Informationen über die üblicherweise von den Arbeitnehmer*innen genutzten Informationssysteme leicht zugänglich gemacht werden. Die konkrete Umsetzung dieser Anforderungen hängt davon ab, unter welchen Umständen die Daten verarbeitet werden. Die DSGVO schreibt zwar keine bestimmte Modalität vor, aber sie verlangt von den Arbeitgeber*innen, »angemessene Maßnahmen zu ergreifen«, die ihren Datenverarbeitungspraktiken entsprechen. Gewerkschaften und Betriebsräte sollten die Initiative ergreifen, wenn es darum geht, wie diese Anforderungen in der Praxis umgesetzt werden können.

iv. **Wie Arbeitnehmer*innen ihre Datenrechte ausüben können:** Einfach nur anzugeben, dass Daten verarbeitet werden, erfüllt die DSGVO-Anforderungen an Fairness und Transparenz nicht vollständig und hilft den Arbeitnehmer*innen auch nicht, ihre Rechte auszuüben. Arbeitgeber*innen müssen nicht nur konkrete Informationen in der vorgegebenen Art, Weise und Zeit angeben, sondern haben auch die positive Verpflichtung, den Arbeitnehmer*innen die Ausübung ihrer Rechte zu ermöglichen. Deswegen müssen Arbeitgeber*innen den Arbeitnehmer*innen eine Zusammenfassung ihrer Datenrechte zur Verfügung stellen und darlegen, was sie tun können, um die jeweiligen Rechte auszuüben. Diese Zusammenfassung ihrer Rechte sollte getrennt von den oben aufgeführten Informationskategorien bereitgestellt werden. Arbeitgeber*innen sollten ihre Arbeitnehmer*innen zum Beispiel ausdrücklich darauf hinweisen, dass sie das Recht haben, der Verarbeitung ihrer personenbezogenen Daten jederzeit zu widersprechen. Diese Information an sich reicht jedoch nicht aus. Die Arbeitnehmer*innen müssen auch darüber aufgeklärt werden, wie sie dieses Recht ausüben können. Gewerkschaften und Betriebsräte sollten wesentlich dazu beitragen, die in der DSGVO und in Kollektivvereinbarungen festgelegten konkreten Datenrechte von Arbeitnehmer*innen zu ermitteln und sicherzustellen, dass alle Arbeitnehmer*innen ausdrücklich über ihre Rechte und ihre Optionen zur Ausübung dieser Rechte informiert werden.

2.2 DAS RECHT AUF AUSKUNFT ÜBER PERSONENBEZOGENE DATEN

Das Auskunftsrecht (Art. 15 DSGVO) ermöglicht es den Arbeitnehmer*innen, eine Kopie ihrer personenbezogenen Daten, die ihr/e Arbeitgeber/in über sie verarbeitet, anzufordern und zu erhalten. Dieses Recht soll die Transparenz erhöhen und den Arbeitnehmer*innen vermitteln, wie und warum ihre Daten verwendet werden, sodass sie sich von der Rechtmäßigkeit der Verarbeitung überzeugen können. Es geht jedoch auch mit gewissen Einschränkungen einher und könnte von den Arbeitgeber*innen als Vorwand genutzt werden, um den Arbeitnehmer*innen Informationen vorzuenthalten. Das Auskunftsrecht kann zum Beispiel zum Schutz der Rechte und Freiheiten anderer beschränkt werden. Arbeitgeber*innen können auch Ausnahmen zum Schutz des geistigen Eigentums oder von Geschäftsgeheimnissen geltend machen, um das Auskunftsrecht von Arbeitnehmer*innen einzuschränken oder zu verweigern. Das ist eine besondere Herausforderung: Daten, die von den Arbeitnehmer*innen im Rahmen ihrer Arbeit erzeugt werden, könnten in geschäftliche Informationen eingebunden werden, weshalb der/die Arbeitgeber/in möglicherweise unternehmerische Interessen und Geschäftsgeheimnisse geltend macht. Gewerkschaften und Betriebsräte können in Kollektivvereinbarungen spezielle Informationskategorien festlegen, die nicht als »geschützt« gelten, um die Rechtssicherheit zu verbessern und sicherzustellen, dass solche Ausnahmen nicht von den Arbeitgeber*innen ausgenutzt werden – absichtlich oder versehentlich. In Kollektivvereinbarungen können auch Vorkehrungen wie das Redigieren einzelner vertraulicher Wörter festgelegt werden, damit die Arbeitgeber*innen vertrauliche Informationen schützen und gleichzeitig das Recht der Arbeitnehmer*innen auf Auskunft über ihre personenbezogenen Daten erfüllen können. Des Weiteren können Arbeitgeber*innen das Auskunftsrecht ablehnen oder begrenzen, wenn eine Arbeitskraft übermäßig viele Anträge stellt.

Gemäß Erwägungsgrund 63 DSGVO können Arbeitgeber*innen die Arbeitnehmer*innen auffordern, die Daten oder Verarbeitungstätigkeiten, über die sie Auskunft haben wollen, zu präzisieren. Diese Bestimmung könnte das Auskunftsrecht erheblich beeinträchtigen, da sie voraussetzt, dass Arbeitnehmer*innen alle von ihren Arbeitgeber*innen verwendeten Kategorien personenbezogener Daten und Verarbeitungsaktivitäten kennen, was in der Realität meist nicht der Fall ist. Gewerkschaften und Betriebsräte könnten einen wichtigen Beitrag zur wirksamen Umsetzung des Auskunftsrechts leisten. Außerdem können und sollten Gewerkschaften und Betriebsräte Kollektivvereinbarungen mit vorteilhafteren Bestimmungen für die Auskunft über personenbezogene Daten aushandeln. Sie sollten sich auch darum bemühen, am Arbeitsplatz eindeutige Vorgehensweisen und Richtlinien bezüglich Datenauskunftsanfragen einzuführen, um sicherzustellen, dass diese Anfragen effizient und DSGVO-Konform bearbeitet werden.

2.3 VERHANDLUNGEN ÜBER KOLLEKTIVE DATENAUSKUNFTS- UND INFORMATIONSRECHTE

Eine der zentralen Aufgaben der Arbeitnehmervertretungen besteht darin, durch den sozialen Dialog die Privilegien der Arbeitgeber*innen zu kompensieren und kollektive Risiken und Schäden abzuwenden. Da bei Datenschutzgesetzen wie

der DSGVO jedoch die Rechte des Einzelnen im Mittelpunkt stehen, können solche Gremien bei diesen Angelegenheiten auf kollektiver Ebene nur bedingt etwas bewirken. Die in der DSGVO und den Gesetzen der Mitgliedstaaten vorgesehenen Schutzmaßnahmen sind zwar maßgeblich, reichen aber im Hinblick auf die kollektiven Risiken durch neue Technologien und Verarbeitungstätigkeiten nicht aus. Folglich müssen Gewerkschaften und Betriebsräte neue kollektive Datenrechte aushandeln und die in den nationalen Gesetzen und Verfahren vorgesehenen Schutzmaßnahmen einschließlich der Mitbestimmungsrechte ausweiten. Dabei sollten sie mindestens die folgenden Aspekte angehen:

i. **Einführung eines kollektiven Informationsrechts:** Durch die Ausweitung des DSGVO-Rechts auf Information über die Datenverarbeitung auf Arbeitnehmervertretungen werden der kollektive Charakter der Arbeitsumgebung und die gemeinschaftlichen Auswirkungen der Datenverarbeitungspraktiken gewürdigt. Dadurch wird gewährleistet, dass Arbeitnehmer*innen kollektiv über die Erhebung und Nutzung ihrer Daten informiert werden. Das ist vor allem in Anbetracht der Nutzung neuer, für viele unverständlicher Technologien von Bedeutung. Gewerkschaften und Betriebsräte könnten die Formulierungen aus der DSGVO (Art. 12–15) nutzen, um näher darzulegen, welche Informationen wie und wann an die Arbeitnehmervertretungen übermittelt werden sollten.

ii. **Einführung eines kollektiven Auskunftsrechts:** Arbeitnehmervertretungen müssen direkten Zugang zu Beschäftigungsdaten haben, um ihre »Schutzfunktion« wahrnehmen zu können. Sie können das Informations- und Machtgefälle am Arbeitsplatz ausgleichen, weitere kollektive Rechte ausüben und ihre kollektiven Bedenken äußern, indem sie sich das kollektive Auskunftsrecht zunutze machen. Dieses Recht kann Arbeitnehmervertretungen auch als Organisations- und Machtgewinnungsmittel dienen. Die DSGVO gibt zwar vor, wie, wann und worüber Arbeitnehmer*innen zu informieren sind, aber Gewerkschaften und Betriebsräte sollten darüber hinaus klären und präzisieren, wie diese Anforderungen – vor allem im Hinblick auf algorithmisches Management – umgesetzt werden sollen. Die entsprechenden Rechte auf Auskunft und Information im Zusammenhang mit algorithmischem Management werden nachstehend erläutert.

iii. **Einführung eines Rechts auf kollektive Prozessführung und Beschwerden:** Arbeitnehmervertretungen sollten das Recht aushandeln, kollektive Rechtsstreitigkeiten oder Beschwerdeeinreichungen bei Datenschutzbehörden im Namen von Beschäftigtengruppen zu initiieren (Art. 80 DSGVO). Diese Herangehensweise geht systematische Probleme auf der Systemebene an, anstatt ihre Bewältigung einzelnen Arbeitskräften zu überlassen.

iv. **Abwägung kollektiver und individueller Rechte:** Kollektive Auskunfts- und Informationsrechte sind zwar von entscheidender Bedeutung, um die Einhaltung der Arbeits- und Datenschutzgesetze und -vereinbarungen zu überwachen, aber es muss sichergestellt werden, dass durch diese kollektiven Rechte keine Datenrechte einzelner Arbeitskräfte verletzt werden. Daher sollten personenbezogene Daten von Arbeitnehmer*innen nur in dem Ausmaß an Gewerkschaften und Betriebsräte weitergegeben werden, wie es für die Erfüllung und Kontrolle der Verpflichtungen aus nationalen und kollektiven Vereinbarungen erforderlich ist.

3

STANDARDS FÜR ALGORITHMISCHES MANAGEMENT

Algorithmisches Management erfordert eine eigenständige Regulierung. Gewerkschaften und Betriebsräte müssen den Datenschutzaspekten bei der Nutzung solcher Technologien im Beschäftigungskontext Vorrang einräumen. Sie sollten eindeutige Bestimmungen aushandeln, die zumindest auf die folgenden zentralen Aspekte des algorithmischen Managements eingehen:

i. **Beteiligung der Arbeitnehmer*innen:** Die Arbeitnehmer*innen oder ihre Vertretungen sollten aktiv in alle Phasen algorithmischer Managementsysteme einbezogen werden – vom Erwerb über die Konfiguration und Bereitstellung bis hin zur Weiterentwicklung und Folgenabschätzung.

ii. **Transparente Entwicklung und Implementierung:** Gewerkschaften und Betriebsräte sollten umfassendere Informationen über die Architektur und Funktionsmechanismen dieser Systeme einholen können. Dazu gehören auch Kenntnisse über die wissenschaftliche Grundlage oder »Logik« der Algorithmen, Dateneingaben, Entscheidungsfindungen und wie sie in verschiedenen Szenarien am Arbeitsplatz angewendet werden. Wie in (i) erwähnt, sollten sie sicherstellen, dass der Entwicklungsprozess transparent und, soweit möglich, mit Beteiligung der Arbeitnehmervertretung abläuft. Um die Rechte und Interessen der Arbeitnehmer*innen schützen zu können, müssen Gewerkschaften und Betriebsräte wissen, wie diese Systeme funktionieren, sich verändern und die Arbeitskräfte beeinflussen. Dazu müssen sie unter anderem Einblicke in die Datenerhebung und Analysemethoden erhalten und die Kriterien für beschäftigungsrelevante Entscheidungen kennen. Dadurch können Gewerkschaften und Betriebsräte die ethische Nutzung von Technologien am Arbeitsplatz wirksam überwachen und beeinflussen und dafür sorgen, dass sie den Arbeitnehmer*innen nicht schadet und den gesetzlichen Vorschriften entspricht.

iii. **Ethische Nutzung von KI-Systemen:** Für die Nutzung algorithmischer Managementsysteme in HR-Prozessen wie Einstellungen, Abgleiche, Aufgabenverteilungen, Leistungsbewertungen (einschließlich Beförderungen und Disziplinarmaßnahmen), Überwachungen und bei anderen personellen Entscheidungen sollte es transparente und gerechte Standards geben. Die Nutzung dieser Systeme zu Sanktions- oder Manipulationszwecken einschließlich Vorhersagen über das Verhalten einer Arbeitskraft, die nichts mit den wesentlichen Aufgaben dieser Arbeitskraft zu tun haben; zur Überwachung der Emotionen, Stimmungslage oder Persönlichkeit der Arbeitskraft; und zur Ermittlung, Profilerstellung oder Prognostizierung der Wahrscheinlichkeit, dass Arbeitnehmer*innen ihre gesetzlichen Rechte wahrnehmen, sollte verboten werden. Außerdem sollte es verboten sein, vollständig automatisierte Entscheidungen über Entlassungen zu treffen.

iv. **Überprüfung des Algorithmus:** Gewerkschaften und Betriebsräte müssen sich für das Recht auf Überprüfung der am Arbeitsplatz verwendeten Algorithmen einsetzen, um sicherzustellen, dass diese den rechtlichen und ethischen Standards entsprechen.

v. **Minderung von Risiken für die Gesundheit und Sicherheit am Arbeitsplatz (OSH):** In Bezug auf die Handhabung von OSH-Risiken einschließlich psychosozialer Risiken wie Diskriminierung, Dequalifizierung, Arbeitsintensivierung oder -beschleunigung, Verletzungen der Privatsphäre und einer unangemessen kompetitiven oder sogar toxischen Kultur am Arbeitsplatz, die auf algorithmisches Management zurückzuführen sind, sollten eindeutige Bestimmungen ausgehandelt werden (ausführlichere Informationen hierzu finden sich in Cefaliello et al. 2023; Faragher 2019; Staab und Geschke 2019).

vi. **Erweiterung der Schutzvorkehrungen aus der Richtlinie zur Plattformarbeit:** Die Richtlinie zur Plattformarbeit kann Gewerkschaften und Betriebsräten bei der Anwendung der Schutzmaßnahmen aus Art. 22 DSGVO im Beschäftigungskontext als Orientierungshilfe dienen. Diese Richtlinie sorgt für eine bessere Rechtsklarheit hinsichtlich automatisierter Entscheidungssysteme und geht sowohl auf vollautomatische als auch halbautomatische Prozesse ein. Die Richtlinie zur Plattformarbeit führt die Transparenzforderungen aus der DSGVO (Art. 13 Abs. 2 Bst. f, Art. 14 Abs. 2 Bst. g und Art. 15 Abs. 1 Bst. h) weiter aus und verpflichtet die Arbeitgeber*innen, ihre Algorithmen so darzulegen, dass sie von den Arbeitnehmer*innen, ihren Vertretungen und den Arbeitsbehörden verstanden

und nachvollzogen werden können. Außerdem verbietet sie die Verarbeitung personenbezogener Daten, die in keinem Bezug zur Arbeitsleistung stehen, und jeglicher Daten zum emotionalen oder psychischen Zustand von Arbeitnehmer*innen. Die Richtlinie schreibt Folgenabschätzungen für diese Systeme vor und garantiert das Recht auf Erläuterungen und Überprüfungen wichtiger Entscheidungen. Gewerkschaften und Betriebsräte sollten sich dafür einsetzen, dass diese Schutzmaßnahmen auf alle Arbeitsumfelder ausgeweitet werden, um einen einheitlichen Schutz der Würde, Interessen und Rechte von Arbeitnehmer*innen zu gewährleisten – unabhängig von der Rechtsnatur des Beschäftigungsverhältnisses.

vii. **Klärung von Schutzvorkehrungen gegen automatisierte Entscheidungen:** Für die Definition, was genau eine wichtige automatisierte Entscheidung im Sinne der DSGVO darstellt, sollten Leitlinien erarbeitet werden. Gewerkschaften und Betriebsräte sollten klare Vorgaben äußern, wie die Schutzvorkehrungen aus Art. 22 DSGVO einschließlich des Rechts auf Erwirkung des Eingreifens einer Person, auf Darlegung des eigenen Standpunkts, auf Anfechtung der Entscheidung und auf Erhalt einer Erklärung der erzielten Entscheidung im Beschäftigungskontext auszulegen sind. Der nötige Umfang der Erklärung hängt beispielsweise vom Kontext, der Schwere und den Konsequenzen ab. Gewerkschaften und Betriebsräte sind gut aufgestellt, um individuelle Einblicke in solche Situationen zu bieten.

4

ASPEKTE DER DURCHSETZUNG

Die Durchsetzung der DSGVO gestaltet sich vor allem im Beschäftigungskontext schwierig: Den Datenschutzbehörden fehlt es oftmals an den nötigen Ressourcen und Fachkenntnissen, um die Datenschutzvorgaben am Arbeitsplatz wirksam durchzusetzen. Wenn automatisierte Überwachung und Entscheidungsfindung sich mit Datenschutz-, Arbeits- und Sozialschutzgesetzen überschneiden, tritt das Problem noch deutlicher zutage.

Gewerkschaften und Betriebsräte sollten sich für die Einführung von Durchsetzungsmechanismen in Absprache mit den verschiedenen Aufsichtsbehörden einsetzen, um in diesem Bereich für eine wirksamere Durchsetzung zu sorgen. Die Richtlinie zur Plattformarbeit skizziert einen kooperativen Rechtsrahmen und unterstützt diese Herangehensweise. Sie teilt die Verantwortlichkeiten auf zwischen den Datenschutz- und den Arbeitsbehörden und sieht einen Austausch maßgeblicher Informationen in Bezug auf ihre jeweiligen regulatorischen Aufgaben vor. Es ist von entscheidender Bedeutung, dass Gewerkschaften und Betriebsräte in diesen Prozess einbezogen werden.

Außerdem sollten sich Gewerkschaften und Betriebsräte unbedingt aktiv an der Durchsetzung von Datenschutzbestimmungen im Arbeitsumfeld beteiligen. Eine solche Beteiligung würde die rechtliche Position der Gewerkschaften und Betriebsräte bei Durchsetzungsfragen stärken.

REFERENZEN

Abraha, Halefom (2023). »Automated Monitoring in the Workplace and the Search for a New Legal Framework: Lessons from Germany and Beyond« (8. Oktober 2023). Abrufbar bei SSRN: https://ssrn.com/abstract=4595760.

Adams-Prassl, Jeremias und andere (2023). »Regulating Algorithmic Management: A Blueprint«, 14 European Labour Law Journal 124.

Custers, Bart und Heijne, Anne-Sophie (2022). »The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in Theory and Practice«, 46 Computer Law & Security Review 105727.

Hießl, Christina (2023). »Jurisprudence of National Courts in Europe on Algorithmic Management at the Workplace«, Europäisches Kompetenzzentrum (ECE) für Arbeitsrecht, Beschäftigungs- und Arbeitsmarktpolitik.

Bagdi, Katalin (2019). »The works council as an independent data controller« (auf Ungarisch). Protokolle aus dem 16. Rechts-Workshop, 2019. https://doi.org/10.24169/DJM/2019/1-2/1.

Cefaliello et al. (2023). »Making algorithmic management safe and healthy for workers: addressing psychosocial risks in new legal provisions«, European Labour Law Journal, 2023, insbes. S. 197–200.

Faragher, Jo (2019). »Zalando accused of misusing software to rank workers«, Personnel Today. https://www.personneltoday.com/hr/zalando-accused-of-misusing-software-to-rank-workers/.

Groß, Torsten (2019). Deutschland: »Works Council's Right To Information In Relation To Sensitive Personal Employee Data« Mondaq, 10. September 2019. https://www.mondaq.com/germany/data-protection/843698/works-councils-right-to-information-in-relation-to-sensitive-personal-employee-data.

Lamken, Tessa (2022). »Works council as data protection law controller?« Externer Datenschutzbeauftragter Dresden, 19. Juni 2022. https://externer-datenschutzbeauftragter-dresden.de/en/data-protection/works-council-as-responsible-party-in-data-protection-law.

Landesdatenschutzbeauftragte Niedersachsen. Thiel (2023). »Das allgemeine Persönlichkeitsrecht der Mitarbeiterinnen und Mitarbeiter überwiegt unternehmerische Interessen«. https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/thiel-das-allgemeine-persoenlichkeitsrecht-der-mitarbeiterinnen-und-mitarbeiter-uberwiegt-unternehmerische-interessen-219596.html.

Staab und Geschke (2019). »Ratings als arbeitspolitisches Konfliktfeld: das Beispiel ZONAR, Hans-Böckler-Stiftung. https://www.boeckler.de/de/boeckler-impuls-zalando-beschaeftigte-im-bewertungsstress-18789.htm.

Stein et al. (2023). »You are you and the app. There's nobody else. Building Worker-Designed Data Institutions within Platform Hegemony« (CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, April 2023). https://doi.org/10.1145/3544548.3581114.

Stepanova, Olga (2022). »Works councils and data protection: a complex relationship in Germany« LinkedIn Pulse, 6. November 2022. https://www.linkedin.com/pulse/works-councils-data-protection-complex-relationship-olga-stepanova.

Stogov, Christina (2022). »The new Section § 79a of the Works Council Constitution Act (BetrVG): Support obligations of the works council in complying with data protection regulations.« Vangard News & Analysis (Blog), April 2022. https://vangard.de/en/news-analysis/blog/the-new-79a-betrvg-support-obligations-of-the-works-council.

Verwaltungsgericht Hannover (2023). »Datenerhebung bei Amazon in Winsen ist rechtmäßig« https://www.verwaltungsgericht-hannover.niedersachsen.de/aktuelles/pressemitteilungen/datenerhebung-bei-amazon-in-winsen-ist-rechtmassig-219664.html.

ÜBER DEN AUTOR

Halefom H. Abraha ist Assistenzprofessor im Fachbereich für internationales und europäisches Recht der juristischen Fakultät der Universität Utrecht. Zu seinen Lehr- und Forschungsschwerpunkten gehören KI-Regulierung, algorithmisches Management im Arbeitsumfeld und Datenschutz. Außerdem erforscht er den länderübergreifenden Datenzugriff im Strafverfolgungskontext und digitale Souveränität. Nach seiner Promotion forschte Dr. Abraha am Bonavero Institute of Human Rights an der Universität Oxford. Er berät Regierungen und internationale Organisationen, darunter den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europaparlaments, in verschiedenen Bereichen digitaler Technologien und der öffentlichen Ordnung.

Danksagung
Vielen Dank an Dr. Michael »Six« Silberman für seine Hilfe beim Verfassen dieser Abhandlung. Außerdem wurde diese Arbeit durch den Europäischen Forschungsrat im Rahmen des EU-Rahmenprogramms für Forschung und Innovation »Horizon 2020« (Finanzhilfevereinbarung Nr. 947806) unterstützt.

IMPRESSUM

Herausgeberin: Friedrich-Ebert-Stiftung |
Competence Centre on the Future of Work |
Cours Saint Michel 30e | 1040 Brüssel | Belgien

Dr. Tobias Mörschel, Direktor des Friedrich-Ebert-Stiftung Competence Centre on the Future of Work

Inhaltliche Verantwortung: Justin Nogarede
justin.nogarede@fes.de

Für mehr Informationen über das
Competence Centre on the Future of Work,
siehe: **https://futureofwork.fes.de/**

Design/Typesetting: pertext, Berlin | www.pertext.de

ISBN 978-3-98628-671-2

www.fes.de/bibliothek/fes-publikationen