Juni 2024

Besserer Datenschutz am Arbeitsplatz

Herbeiführung DSGVO-konformer Arbeitsumgebungen, Präzisierung nationaler arbeitsbezogener Datenschutzvorschriften und Verbesserung des Datenschutzes für Arbeitskräfte durch Sozialdialog

Justin Nogarede, Michael 'Six' Silberman, und Joanna Bronowicka

Arbeitnehmer*innenrechte im digitalen Zeitalter

FRIEDRICH EBERT STIFTUNG

ARBEITNEHMER*INNENRECHTE IM DIGITALEN ZEITALTER

BESSERER DATENSCHUTZ AM ARBEITSPLATZ

Herbeiführung DSGVO-konformer Arbeitsumgebungen, Präzisierung nationaler arbeitsbezogener Datenschutzvorschriften und Verbesserung des Datenschutzes für Arbeitskräfte durch Sozialdialog

Inhalt

ZUSAMMENFASSUNG

Die Einhaltung geltender Datenschutzgesetze am Arbeitsplatz gilt als mangelhaft. Dafür gibt es verschiedene Gründe, unter anderem die rechtliche Unklarheit und die unzureichende Mittelausstattung von Arbeitnehmerorganisationen (wie Gewerkschaften), Datenschutzbeauftragten und -behörden.

Diese Abhandlung zeigt auf, wie Sozialpartner, Regierungen und Organisationen der Zivilgesellschaft die Einhaltung des Datenschutzes am Arbeitsplatz verbessern können. Dabei geht es vor allem um folgende Themen:

1. Die bestehenden Datenschutzgesetze bieten Sozialpartnern und den nationalen Regierungen bereits zahlreiche Möglichkeiten, die bislang noch nicht völlig ausgeschöpft wurden. Diese Möglichkeiten, zu denen auch Verhaltensregeln und Zertifizierungssysteme gemäß den Artikeln 40 und 42 DSGVO gehören, könnten bislang unklare Aspekte in der Datenschutzgesetzgebung spezifizieren und die Datenschutzbehörden in Durchsetzungsangelegenheiten entlasten.

2. Die Mitgliedstaaten sollten mithilfe von Artikel 88 DSGVO nationale Datenschutzvorschriften für den Beschäftigungskontext erlassen – und dabei von den Sozialpartnern und Organisationen der Zivilgesellschaft unterstützt werden. Die aktuellen rechtlichen Entwicklungen auf EU-Ebene haben die Anforderungen an nationale Gesetze gemäß Art. 88 verdeutlicht. Dadurch bietet sich den Mitgliedstaaten die Gelegenheit, für mehr rechtliche Klarheit hinsichtlich der Anwendung geltender Datenschutzvorschriften im Beschäftigungskontext zu sorgen, zusätzliche maßgebliche Schutzmaßnahmen einzuführen und die Einhaltung und Durchsetzung der Gesetze zu verbessern.

3. Sachverständige können Gewerkschaften und Datenschutzbehörden bei der Überprüfung algorithmischer Systeme unterstützen. Die Komplexität und Undurchschaubarkeit arbeitsbezogener Datenverarbeitungssysteme und -praktiken erfordert technische Einblicke und Fachkenntnisse zur Beurteilung, ob diese Systeme und Praktiken den geltenden Gesetzen entsprechen.

4. Strategische Rechtsverfahren können rechtliche Unsicherheiten ausräumen und als finanziell unangenehme Abschreckungsmaßnahme gegen Verstöße dienen. Solche Prozesse haben sich bei der Verarbeitung von Verbraucherdaten als äußerst hilfreich erwiesen. Nun gilt es herauszufinden, welches Potenzial sie bei der arbeitsbezogenen Datenverarbeitung haben.

In dieser Abhandlung gehen wir auf diese Themen ein, nennen konkrete Beispiele und verweisen bei Bedarf auf die entsprechende Literatur.

EINLEITUNG

Beim Experten-Workshop des Kompetenzzentrums »Zukunft der Arbeit« der Friedrich-Ebert-Stiftung (FES) am 19. Oktober 2023 in Brüssel ging es um den aktuellen Stand der Datenschutzkonformität und -durchsetzung im Beschäftigungskontext. Daran nahmen politische Entscheidungsträger*innen einschließlich nationaler und regionaler Datenschutzbeauftragter und Amtsleute der Europäischen Kommission, aber auch Fachleute aus der Praxis wie Gewerkschaftsvertreter*innen und Sachverständige aus Organisationen der Zivilgesellschaft sowie Wissenschaftler*innen, die sich aktiv mit diesem Thema befassen, teil.

Bei den Gesprächen stand die übergeordnete Aufgabe des FES-Kompetenzzentrums »Zukunft der Arbeit« im Mittelpunkt: Wie lässt sich eine europäische Wirtschaft mit angemessenen Arbeitsbedingungen, Chancengleichheit und sozialer Sicherheit für alle angesichts der rasanten Ausbreitung digitaler Technologien in der Arbeitswelt bewerkstelligen? Fortschrittliche digitale Technologien können zwar die Produktivität und Wettbewerbsfähigkeit Europas verbessern, aber sie müssen vom Sozialdialog geprägt sein und sich am Rechtsrahmen orientieren, um sicherzustellen, dass die digitale Transformation die europäische Verpflichtung zur Sozialpartnerschaft und den grundlegenden Menschenrechten nicht untergräbt, sondern unterstützt und verstärkt.

Vor allem die Datenschutzgesetze spielen eine entscheidende Rolle für die Richtung der digitalen Transformation, auch am Arbeitsplatz. Die schiere Menge der bei den Datenschutzbehörden eingereichten Beschwerden hat jedoch erhebliche Schwierigkeiten bei der Durchsetzung zur Folge. Das ist auch den Behörden, dem Europäischen Datenschutzausschuss und dem europäischen Gesetzgeber bewusst. Am 7. April 2023 schlug die Kommission sogar eine neue Verordnung zur Bewältigung der Durchsetzungsschwierigkeiten speziell bei länderübergreifenden Fällen vor (der Vorschlag für eine »Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679«).

Die technische und organisatorische Komplexität der Datenverarbeitung im Arbeitsumfeld stellt aber nicht nur die Datenschutzbehörden, sondern auch die Sozialpartner vor besondere Herausforderungen. Vor allem Gewerkschaften versuchen, die Arbeitgeber*innen zur Einhaltung der Datenschutzvorschriften anzuregen und diese zu gewährleisten. In Verbindung mit der Rechtsunsicherheit bezüglich bestimmter Schlüsselbegriffe und Konzepte in den geltenden Datenschutzgesetzen – zum Beispiel, wo die Grenzen der »berechtigten Interessen« von Datenverantwortlichen liegen und welche Bedingen erfüllt sein müssen, damit die Einwilligung der Datensubjekte wirklich als »freiwillig erteilt« gilt – stellt diese Komplexität selbst die Arbeitgeber*innen, die sich an die Vorschriften halten *wollen*, vor Herausforderungen.

Forscher*innen, Datenschutzbehörden und Sozialpartner fordern schon seit Jahren nationale Gesetze für den Datenschutz im Beschäftigungskontext, um diese Probleme zumindest teilweise anzugehen, aber bislang hat sich kein einziger Mitgliedstaat eingehend damit befasst. Bei diesem Workshop sollten auch die Fortschritte bei diesen großen Herausforderungen erörtert und mögliche Maßnahmen durch die Sozialpartner, zivilgesellschaftlichen Akteur*innen, Mitgliedstaaten und EU-Institutionen dargelegt werden.

Anfang 2024 verabschiedete die EU die Richtlinie zur Plattformarbeit und den »AI Act« (KI-Gesetz). Beide spielen für die Datenverarbeitung im Arbeitsumfeld eine wichtige Rolle. Als der Workshop stattfand, waren diese Gesetze allerdings noch Gegenstand intensiver Verhandlungen, und ihre Vorteile und Defizite werden erst in den nächsten Jahren vollständig zutage treten. Daher geht es in dieser Publikation vor allem um die (unzureichende) Einhaltung der Datenschutz-Grundverordnung (DSGVO) – ein horizontales Gesetz, das die Verarbeitung personenbezogener Daten aller Arbeitskräfte in der EU, unabhängig von ihrem Vertragsstatus, regelt, von den Mitgliedstaaten implementiert wurde und seit nunmehr fast sechs Jahren in Kraft ist.

Aus der Diskussion ergaben sich fünf Themenschwerpunkte:

1. **Die Einhaltung geltender Datenschutzgesetze am Arbeitsplatz gilt als mangelhaft**, und die Workshop-Teilnehmer*innen hielten eine baldige Besserung der Situation für unwahrscheinlich.

2. **Die bestehenden Datenschutzgesetze bieten Sozialpartnern und den nationalen Regierungen bereits zahlreiche Möglichkeiten, die bislang noch nicht völlig ausgeschöpft wurden.** Abgesehen von Artikel 88, nach dem die Mitgliedstaaten landesspezifi-

sche Datenschutzvorschriften für den Beschäftigungskontext erlassen können, ermöglicht die DSGVO es den Datenverantwortlichen und anderen Beteiligten zudem, freiwillige Verhaltensregeln (Art. 40) und Zertifizierungssysteme (Art. 42) einzuführen. Freiwillige Systeme können zwar verbindliche Gesetze und deren angemessene Durchsetzung nicht ersetzen, aber durchaus als Möglichkeit genutzt werden, rechtliche Unsicherheiten zu klären und die Konformität bei den »wohlgesinnten« Datenverantwortlichen zu verbessern. Zusätzlich zu den freiwilligen Systemen können die Mitgliedstaaten gemäß Art. 80 Abs. 2 DSGVO auch Organisationen der Zivilgesellschaft ermächtigen, Datenschutzbeschwerden ohne Einzelmandat (»Initiativbeschwerden«) einzureichen. Bislang haben aber nur wenige Mitgliedstaaten von dieser Möglichkeit Gebrauch gemacht.

3. **Die Mitgliedstaaten sollten mithilfe von Artikel 88 DSGVO nationale Datenschutzvorschriften für den Beschäftigungskontext erlassen – und dabei von den Sozialpartnern und Organisationen der Zivilgesellschaft unterstützt werden.** Die aktuellen rechtlichen Entwicklungen auf europäischer Ebene haben die Anforderungen an Gesetze gemäß Art. 88 verdeutlicht. Diese Anforderungen sind streng, und die Mitgliedstaaten sollten sie sorgfältig ausarbeiten, damit sie später nicht für ungültig erklärt werden. Wissenschaftliche Recherchen und Vorschläge von zivilgesellschaftlichen Organisationen haben verdeutlicht, wie diese Gesetze inhaltlich gestaltet werden sollten.

   Theoretisch könnte eine EU-Richtlinie als transnationaler Rahmen für den Datenschutz im Arbeitsumfeld dienen. Angesichts der drohenden Fragmentierung durch die erheblich voneinander abweichenden nationalen Vorschriften wäre ein solcher Rahmen wünschenswert. Die politischen Aussichten für eine derartige Richtlinie sind jedoch zweifelhaft. Folglich stand für die meisten Workshop-Teilnehmer*innen die Einführung nationaler Vorschriften im Vordergrund.

4. **Sachverständige können Gewerkschaften und Datenschutzbehörden bei der Überprüfung algorithmischer Systeme unterstützen.** Solche Überprüfungen sind sogar dann möglich, wenn die Plattformen nicht willens oder in der Lage sind, Transparenz bezüglich der Erhebung oder Verarbeitung der Beschäftigtendaten zu schaffen, um mögliche Verstöße gegen die DSGVO zu verbergen. Sachverständige erkunden derzeit verschiedene Methoden zur Ermittlung von DSGVO-Verstößen einschließlich Analysen der Daten, die von Unternehmen über Auskunftsanfragen eingeholt wurden. Dabei wenden sie Datenextraktionsmethoden oder »Black-Box-Analysen« an.

5. **Strategische Rechtsverfahren können rechtliche Unsicherheiten ausräumen und als finanziell unangenehme Abschreckungsmaßnahme gegen Verstöße dienen.** Dazu dient die Arbeit von Max Schrems und seiner Organisation NYOB im Hinblick auf den Verbraucherdatenschutz als Vorbild. Zur Unterstützung rechtlicher Initiativen für den Datenschutz im *Beschäftigungskontext* könnte eine ähnliche Organisation gegründet werden.

In dieser Abhandlung geht es um diese Themen, die nächsten Schritte für die Sozialpartner, Forscher*innen und Akteur*innen der Zivilgesellschaft.

1

HERAUSFORDERUNGEN BEI DER KONFORMITÄT UND DURCHSETZUNG

Mehreren Workshop-Teilnehmer*innen zufolge sind die Unternehmen oft nicht willens oder in der Lage, den Informations- oder Zugriffsanfragen der Arbeitskräfte nachzukommen, da sie keine genauen und vollständigen Aufzeichnungen über die Verarbeitung von Beschäftigtendaten pflegen. Außerdem führen sie oft keine Datenschutz-Folgenabschätzungen durch und sind meist auf (äußerst kostspielige) Software angewiesen, die nicht die nötige Transparenz und Nutzerkontrolle (also Löschung von Daten) zur Einhaltung der DSGVO-Bestimmungen bietet.

Zudem halten die Unternehmen laut den Teilnehmer*innen die DSGVO oft nicht ein, weil ihnen der Anreiz dazu fehlt: Um Software und Geschäftspraktiken DSGVO-konform zu gestalten, müssen umgehend Zeit und Mittel in großem Umfang investiert werden. Die Risiken bei einer Nichteinhaltung hingegen sind ungewiss und eher gering. In der Praxis können Datenschutzbehörden nur auf Beschwerden reagieren. Arbeitskräfte scheuen aber angesichts des Machtgefälles am Arbeitsplatz oft davor zurück, solche Beschwerden einzureichen. Oder, wie es ein Teilnehmer ausdrückte: »Arbeitskräfte, die ihre Datenrechte gemäß DSGVO wahrnehmen, werden als Feinde des Unternehmens angesehen.« Und selbst wenn Beschwerden bei den Datenschutzbehörden eingehen, ergreifen diese nur in sehr wenigen Fällen Durchsetzungsmaßnahmen und verhängen abschreckende Bußgelder.

Hinzu kommt, dass Gewerkschaften und Betriebsräte nicht über die nötigen Fachkenntnisse und Ressourcen verfügen, um die mitunter abstrakten Rechtsgrundsätze im konkrete Kollektiv- oder Firmenvereinbarungen für die Datenverarbeitung am Arbeitsplatz umzuwandeln, und dadurch Arbeitgeber*innen und Plattformen nicht zwingen können, die DSGVO ernstzunehmen. Unzureichende Fachkenntnisse sind auch für die Firmen – vor allem für kleine und mittelständische Unternehmen – ein Problem.

Nicht zuletzt schenken sowohl Arbeitnehmervertretungen als auch die Arbeitskräfte selbst dem Datenschutz und der Data Governance nicht die gebührende Aufmerksamkeit. In erster Linie betrachten sie diese Aspekte aus der Perspektive der individuellen Privatsphäre, anstatt zu bedenken, dass Datenströme sich zunehmend auf die allgemeinen Arbeitsbeziehungen (Autonomie, Sanktionen, Prämien, Wettbewerbsdynamik) auswirken. Die Datenverarbeitung beeinflusst also nicht nur die Arbeitsbedingungen der Beschäftigten, sondern auch die Machtverhältnisse zwischen Arbeitgeber*innen und Arbeitnehmer*innen (siehe u. a. Adams und Wenckebach 2023; Calacci und Stein 2023).

2

UNZUREICHEND AUSGESCHÖPFTE OPTIONEN IN DER DATENSCHUTZGESETZGEBUNG

In diesem Abschnitt geht es um fünf in der DSGVO aufgeführte, bislang kaum genutzte Möglichkeiten, die den Datenschutz im Arbeitsumfeld verbessern könnten. Abschnitt 2.1 geht kurz ein auf Art. 88 DSGVO, der es den Mitgliedstaaten ermöglicht, zusätzliche, auf den Arbeitsplatz bezogene Datenschutzvorschriften festzulegen. Die jüngsten rechtlichen Entwicklungen bezüglich solcher Vorschriften gemäß Artikel 88 sowie Inhaltsempfehlungen für diese Vorschriften werden ausführlich in der hiermit einhergehenden Publikation »Stärkung der Datenschutzrechte von Arbeitnehmer*innen« von Halefom Abraha erörtert.

In Abschnitt 2.2 geht es um die in Art. 80 Abs. 2 DSGVO erwähnten Möglichkeiten für die Mitgliedstaaten, das Recht zur Einreichung von Beschwerden bei den Datenschutzbehörden auch ohne ausdrückliches Mandat von unmittelbar betroffenen Datensubjekten auf gemeinnützige Organisationen wie Gewerkschaften und Verbraucherverbände zu übertragen.

Abschnitt 2.3 stellt Art. 25 DSGVO (»Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen«) vor. Dieser Artikel verlangt von den Datenverantwortlichen, »geeignete technische und organisatorische Maßnahmen« zu treffen, um die Datenschutzgrundsätze wirksam umzusetzen, und geht auf die mögliche Bedeutung für den Beschäftigungskontext ein.

Abschnitt 2.4 behandelt die Artikel 40 und 41 DSGVO. Diese Bestimmungen ermöglichen es Vertretungen von Datenverantwortlichen, freiwillige Verhaltensregeln zur weiteren Konkretisierung der Bedeutung von DSGVO-Grundsätzen unter bestimmten Umständen einzuführen. Die »Verarbeitung personenbezogener Beschäftigtendaten durch den/die Arbeitgeber/in« könnte ein solcher Umstand sein.

Abschließend beleuchtet Abschnitt 2.5 die Artikel 42 und 43 DSGVO in Bezug auf die Einrichtung von Datenschutz-Zertifizierungssystemen.

2.1 ARTIKEL 88 DSGVO: LANDESSPEZIFISCHE VORSCHRIFTEN FÜR DEN DATENSCHUTZ IM BESCHÄFTIGUNGSKONTEXT

Art. 88 DSGVO räumt den Mitgliedstaaten die Möglichkeit ein, »spezifischere Vorschriften [...] hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext« vorzusehen. Diese Vorschriften können in nationalen Gesetzen oder Kollektivvereinbarungen einschließlich Arbeitsvereinbarungen auf Firmenebene – den sogenannten *Betriebsvereinbarungen* – festgelegt werden. Erwägungsgrund 155 verdeutlicht, dass diese Vorschriften zum Beispiel geeignete Rechtsgrundlagen und Zwecke für die Verarbeitung personenbezogener Beschäftigtendaten darlegen können. Beispiele für Kollektivvereinbarungen über Daten finden sich im Digital Bargaining Hub von Public Services International (PSI).

Art. 88 Abs. 3 DSGVO verpflichtet die Mitgliedstaaten, die Kommission über die entsprechend erlassenen Vorschriften zu informieren. In einer 2022 veröffentlichten juristischen Publikation wurde untersucht, inwieweit die dokumentierte Nutzung dieser Bestimmungen durch die Mitgliedstaaten bis zu diesem Zeitpunkt die zuvor ermittelten Schwierigkeiten beim Datenschutz am Arbeitsplatz in Angriff nahm (Abraha 2022). Damals hatten 17 Mitgliedstaaten beschäftigungsspezifische Datenschutzvorschriften in irgendeiner Form erlassen. Abraha (2022) stellte jedoch fest, dass diese Nutzung zwar »vielfältige und mitunter innovative regulatorische Herangehensweisen« der Mitgliedstaaten zum Erfüllen der Bedürfnisse, die sich aus ihren speziellen arbeitsrechtlichen Gegebenheiten und Beziehungen zwischen Arbeitgeber*innen und Arbeitnehmer*innen ergaben, hervorgerufen hatte, die beschäftigungsspezifischen Vorschriften der Mitgliedstaaten aber scheinbar nicht alle Anforderungen aus Art. 88 Abs. 2 erfüllten.

Gemäß Art. 88 Abs. 2 müssen landesspezifische Vorschriften für den Datenschutz im Beschäftigungskontext »geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf« bestimmte Datenverarbeitungspraktiken enthalten. Abraha hielt fest, dass die Mitgliedstaaten durch ihre vielfältigen Auslegungen des Art. 88 DSGVO eine zunehmende Fragmentierung hinsichtlich der DSGVO-Implementierung und -Durchsetzung am Arbeitsplatz riskierten.

Und tatsächlich ersuchte ein deutsches Verwaltungsgericht 2023 den EuGH in der Rechtssache *Hauptpersonalrat der Lehrerinnen und Lehrer* um eine Vorabentscheidung, ob die Anforderungen aus Art. 88 Abs. 2 DSGVO in den deutschen

Gesetzen erfüllt werden. Der EuGH kam zu dem Schluss, dass dies nicht der Fall sei, da die deutschen Gesetze keine maßgeblichen neuen, arbeitsspezifischen Vorschriften mit »geeigneten und besonderen Maßnahmen« erließen. Dieses Urteil hat das deutsche Gesetz für Art. 88 scheinbar effektiv außer Kraft gesetzt und könnte auch erhebliche Auswirkungen auf die Gesetze anderer Mitgliedstaaten haben (siehe Abraha 2023).

Dieses ziemlich drastische Urteil verschafft den Akteur*innen der Zivilgesellschaft die Gelegenheit, die nationalen Gesetzgeber aufzufordern, angesichts der zunehmenden Datenverarbeitung im Arbeitsumfeld für maßgebliche, zweckdienliche und einschlägige Schutzmaßnahmen für die Arbeitnehmer*innen in neuen nationalen Gesetzen zum Datenschutz im Beschäftigungskontext zu sorgen.

Die hiermit einhergehende Publikation »Stärkung der Datenschutzrechte von Arbeitnehmer*innen« von Halefom Abraha erläutert, für welche konkreten Inhalte sich die Gewerkschaften und – vor allem in Ländern mit begrenzter gewerkschaftlicher Macht und Kapazitäten – andere Akteur*innen der Zivilgesellschaft einsetzen sollten.

2.2 ARTIKEL 80 ABS. 2 DSGVO: »INITIATIVBESCHWERDEN« VON ORGANISATIONEN DER ZIVILGESELLSCHAFT

Laut Art. 80 Abs. 1 DSGVO müssen die Mitgliedstaaten gewährleisten, dass Datensubjekte eine Organisation mit ihrer Vertretung und Einreichung von Beschwerden bei Datenschutzbehörden (Art. 77), der gerichtlichen Anfechtung von Entscheidungen der Behörden (Art. 78) und Einreichungen von Klagen gegen Datenverantwortliche und -verarbeitende bei einer Verletzung ihrer Rechte (Art. 79) beauftragen können. Einzelberichten zufolge schrecken Arbeitskräfte jedoch davor zurück, Organisationen mit dem Einreichen von Beschwerden oder Führen eines Gerichtsprozesses in ihrem Namen zu beauftragen, da sie Vergeltungsmaßnahmen ihrer Arbeitgeber*innen fürchten.

Glücklicherweise sieht Art. 80 Abs. 2 DSGVO vor, dass die Mitgliedstaaten jeder beliebigen gemeinnützigen Organisation, die im Interesse der Öffentlichkeit handelt und die Rechte von Datensubjekten schützt, die Einreichung von Beschwerden bei Datenschutzbehörden und die Einleitung von Rechtsverfahren gegen Datenverantwortliche und -verarbeitende gestatten können – auch ohne Mandate der Betroffenen. Kurz gesagt: Sie können »Initiativbeschwerden« einreichen. Gewerkschaften und andere Organisationen haben so die Möglichkeit, Verwaltungsverfahren einzuleiten oder Rechtsbehelfe für Arbeitskräfte (mit Ausnahme von Entschädigungen) einzufordern, ohne dass diese herausgestellt und den Repressalien ihres Unternehmens ausgesetzt werden.

Darüber hinaus bestätigte der EuGH in der Rechtssache C-319/20 *Meta Platforms Ireland*, dass Organisationen, die die Anforderungen aus Artikel 80 DSGVO und/oder entsprechende nationale Gesetze erfüllen, Ansprüche im kollektiven Interesse der Betroffenen erheben können, ohne beweisen zu müssen, dass die Rechte eines einzelnen Datensubjekts verletzt wurden (also dass ein tatsächlicher Schaden entstanden ist).

Leider hat bislang kein Mitgliedstaat außer vielleicht Dänemark (BEUC 2023) den optionalen Art. 80 Abs. 2 implementiert (siehe u. a. Pato 2019). Allerdings gestatten mehrere Mitgliedstaaten neben Dänemark Sammelklagen im Verbraucherbereich und manchmal auch darüber hinaus. Dazu gehören beispielsweise Frankreich, Belgien, Deutschland, die Niederlande und Spanien.

Weitere Rechtsanalysen zur Klärung, ob und wo Arbeitnehmervertretungen wie Gewerkschaften Ansprüche aus der DSGVO ohne vorheriges Mandat von einzelnen Arbeitskräften erheben, wären wünschenswert.

2.3 ARTIKEL 25 DSGVO: DATENSCHUTZ DURCH TECHNIKGESTALTUNG UND DURCH DATENSCHUTZFREUNDLICHE VOREINSTELLUNGEN

Artikel 25 DSGVO, »Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen«, verlangt von den Datenverantwortlichen, »geeignete technische und organisatorische Maßnahmen« zu treffen, »um die Datenschutzgrundsätze wirksam umzusetzen […] und die Rechte der betroffenen Personen zu schützen«.

Dieser Artikel verankert ein überwiegend technisches oder gestalterisches »Paradigma« für die Datenschutzkonformität im Gesetz, das größtenteils in den Bereich der Softwareentwicklung fällt (siehe z. B. Dewitte 2023).Die möglichen Grenzen einer technischen oder »gestalterischen« Herangehensweise an den Datenschutz für Arbeitnehmer*innen vor dem Hintergrund des maschinellen Lernens, künstlicher Intelligenz oder anderer »selbstlernender« Entscheidungssysteme wurden zwar bereits dokumentiert (u. a. in Cefaliello et al. 2023), aber das bedeutet keineswegs, dass dieser Ansatz nicht zur Verbesserung der Konformität beitragen kann.

Die Leitlinien 4/2019 des Europäischen Datenschutzausschusses zu Artikel 25 weisen sogar darauf hin, dass Artikel 25 den Datenverantwortlichen ziemlich strenge Verpflichtungen im Hinblick auf ihre zur Datenverarbeitung verwendeten Systeme auferlegt. Unter anderem präzisieren die Leitlinien, dass »Auftragsverarbeiter und Hersteller […] hinsichtlich der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als wichtige Akteure [gelten]«, jedoch »**die Verantwortlichen für die Verarbeitung personenbezogener Daten nur Systeme und Techniken mit integriertem Datenschutz verwenden dürfen**« (Paragraph 94, S. 35, eigene Hervorhebung). Diese Anforderung ist dem Anschein nach recht streng, und die Leitlinien des Ausschusses legen ausführlich dar, wie genau der »integrierte Datenschutz« aussehen soll, einschließlich eines Beispiels für die Datenverarbeitung am Arbeitsplatz (S. 26–27).

Aber wie auch bei der DSGVO als Ganzes liegt das Hauptproblem in der Konformität und Durchsetzung. Es ist davon auszugehen, dass zum gegenwärtigen Zeitpunkt ein Großteil der Datenverarbeitung am Arbeitsplatz die Anforderungen aus Art. 25 DSGVO nicht erfüllt (siehe z. B. Christl 2023, insbesondere S. 63; allgemeiner siehe u. a. Christl 2021), und den Datenschutzbehörden und Arbeitnehmervertretungen mangelt es an Möglichkeiten, diese durchzusetzen. Dennoch eröffnet Art. 25 die Möglichkeit, die Konformität durch »einmalige« technische Änderungen in der Gestaltung von »standardmäßigen«, an vielen Arbeitsplätzen verwendeten Softwaresystemen zu verbessern. In weiteren Untersuchungen konnten weitverbreitete Betriebssoftwaresysteme auf ihre Einhaltung der Anforderungen aus Art. 25 gemäß den Ausschussleitlinien bewertet und Möglichkeiten für technische Anpassungen zur Verbesserung der Konformität herausgestellt werden.

Laut Art. 25 Abs. 3 kann die Einhaltung der Anforderungen aus Art. 25 Abs. 1 und 2 mit Zertifizierungsmechanismen gemäß Art. 42 DSGVO nachgewiesen werden. Außerdem regt der Datenschutzausschuss in seinen Leitlinien 4/2019 »alle Verantwortlichen an, von Zertifizierungen und Verhaltensregeln [gemäß Art. 40 DSGVO] Gebrauch zu machen« (S. 5). Daher könnten in weiteren Untersuchungen Möglichkeiten zur Verankerung von »bewährten Datenschutzpraktiken« für Betriebssoftware in Zertifizierungen und Verhaltensregeln erkundet werden.

2.4 ARTIKEL 40 UND 41 DSGVO: VERHALTENSREGELN

Artikel 40 »Verhaltensregeln« und Artikel 41 »Überwachung der genehmigten Verhaltensregeln« DSGVO legen die rechtlichen Rahmenbedingungen für Datenschutz-Verhaltensregeln fest. Diese Verhaltensregeln sind zwar freiwillig, aber die Bestimmungen aus den Artikeln 40 und 41 enthalten klare Vorgaben für den Inhalt solcher Regeln und die Art und Weise der Einhaltungsüberwachung genehmigter Regeln. Sie sind also nicht beliebig anzuwenden, sondern eher als eine Art »regulierte Selbstregulierung« zu betrachten.

Gemäß Art. 40 können »Verbände und andere Vereinigungen, die Kategorien von [Daten]Verantwortlichen oder Auftragsverarbeitern vertreten, [...] Verhaltensregeln ausarbeiten [...]«, mit denen die Anwendung der DSGVO auf ihre konkreten Verarbeitungstätigkeiten präzisiert wird. Verhaltensregeln können die Bedeutung der grundlegenden Konzepte aus der DSGVO für die konkreten Verarbeitungspraktiken der betroffenen Verantwortlichen/Verarbeitenden, z. B. »gerecht und transparent« und »berechtigte Interessen«, präzisieren und einzuhaltende »Standards« oder »bewährte« Vorgehensweisen zur Erfüllung der Datenschutzpflichten angeben. Dazu gehört unter anderen, welche Informationen über die Verarbeitung den Datensubjekten zur Verfügung gestellt und welche Maßnahmen angewendet werden müssen, um die Einhaltung von Art. 25 DSGVO zu gewährleisten (siehe Abschnitt 2.3 oben).

»Arbeitgeber*innen« könnten als eine Kategorie von Datenverantwortlichen und/oder »Anbieter*innen von Software zur Verarbeitung personenbezogener Beschäftigtendaten« als Verantwortliche und/oder Verarbeitende betrachtet werden, um DSGVO-Verhaltensregeln für diese Kategorien von Verantwortlichen/Verarbeitenden festzulegen. In diesem Zusammenhang sollten derartige Regeln auch momentan noch mehrdeutige und umstrittene Begriffe und Fragen in der DSGVO klären, zum Beispiel, was genau »zwingend notwendig« bedeutet und wie die »Verhältnismäßigkeit« der Verarbeitung personenbezogener Beschäftigtendaten definiert wird (z. B. wenn die »berechtigten Interessen« der Arbeitgeber*innen bei der Personaldatenverarbeitung die Datenschutzrechte der Beschäftigten überwiegen könnten oder von diesen aufgewogen werden).

Silberman und Johnston (2020) erörtern die Inhalte der Artikel 40 und 41 im Hinblick auf die Verarbeitung von Beschäftigtendaten (S. 13–14) und betrachten die mit diesen Bestimmungen eingeführten Rahmenbedingungen aus dem Blickwinkel früherer Defizite in Verhaltensregeln, die von Arbeitgeber*innen in globalen Wertschöpfungsketten »selbst entwickelt« wurden (S. 14–16).

Die Akteur*innen der Zivilgesellschaft könnten im nächsten Schritt qualitative Forschungen zu möglichen DSGVO-Verhaltensregeln für Arbeitgeber*innen und/oder Anbieter*innen von Software zur Verarbeitung personenbezogener Beschäftigtendaten mit den entsprechenden Interessengruppen durchführen. Dazu zählen vor allem Arbeitgeber- und Arbeitnehmervertretungen (z. B. durch Interviews und Workshops) sowie Softwareanbieter*innen. Im Zuge dieser Untersuchungen könnten auch Möglichkeiten erforscht werden, um sicherzustellen, dass Arbeitnehmer- und Arbeitgebervertretungen umfassend in die Ausarbeitung, Durchsetzung und Weiterentwicklung dieser Verhaltensregeln einbezogen werden.

2.5 ARTIKEL 42 UND 43 DSGVO: ZERTIFIZIERUNGSSYSTEME

Art. 42 DSGVO befürwortet die Einführung freiwilliger Zertifizierungsmechanismen, um die Einhaltung der Gesetze zu erleichtern und die Transparenz für die Datensubjekte zu erhöhen. Vor allem im Hinblick auf die mangelhafte Durchsetzung ist eine Zertifizierung eine gute Möglichkeit zur Verbesserung der Konformität, da so die Auswirkungen der allgemeinen Datenschutzbestimmungen aus der DSGVO für konkrete Zusammenhänge und Datenverarbeitungsvorgänge spezifiziert werden.

Ein Alleinstellungsmerkmal der DSGVO ist, dass sie vollkommen offen lässt, wer die Zertifizierungskriterien ausarbeiten soll – der wichtigste Aspekt bei einem Zertifizierungssystem. Im Grunde kann also jede Organisation, auch eine Gewerkschaft oder jede andere Rechtsperson, die sich für die Interessen der Arbeitnehmer*innen einsetzt, ein System ausarbeiten. Nachdem die Kriterien ausgearbeitet wurden, müssen sie gemäß Art. 42 und 43 von einer Datenschutzbehör-

de – bzw. bei EU-weiten Systemen vom Europäischen Datenschutzausschuss – genehmigt und anschließend von einer Zertifizierungsstelle oder Datenschutzbehörde zur Zertifizierung von Datenverantwortlichen und -verarbeitenden herangezogen werden (siehe u. a. Kamara & De Hert 2018).

Zertifizierungssysteme außerhalb des Rahmens von Art. 42 und 43 sind jedoch laut DSGVO nicht verboten – und kommen auch zum Einsatz. Diese Systeme profitieren nicht von den unverbindlichen Konformitätsannahmen für Anwender*innen, die z. B. gemäß Art. 42 und 43 zertifiziert wurden (siehe Art. 24 Abs. 3, Art. 25 Abs. 3, Art. 28 Abs. 5 und Art. 32 Abs. 3). Sie profitieren auch nicht von Art. 83 Abs. 2 Bst. j, der gestattet, beim Verhängen von Geldbußen die Einhaltung von DSGVO-gemäßen Zertifizierungssystemen zu berücksichtigen (z. B. durch eine niedrigere Geldbuße).

Das Potenzial, das Zertifizierungen bieten, wurde bislang nur unzureichend ausgeschöpft. Laut dem Verzeichnis des Europäischen Datenschutzausschusses sind derzeit (Stand: Mai 2024) nur vier offiziell zugelassene Zertifizierungssysteme in Betrieb. Dabei handelt es sich um ein europaweites System namens Europrivacy und drei nationale Systeme – jeweils eins in Deutschland, in Luxemburg und in den Niederlanden. Keines davon beschränkt sich auf bestimmte Sektoren oder Verarbeitungsvorgänge, es sind also allgemeine Systeme. Hier herrscht noch großer Nachbesserungsbedarf: Diese Systeme müssen nach wie vor darlegen, wie die DSGVO in einem bestimmten Kontext wie der Verarbeitung von Beschäftigtendaten oder bei bestimmten Vorgängen wie der automatisierten Verarbeitung von Lebensläufen angewendet wird (Von Grafenstein 2021).

Daher sollte die Ausarbeitung von Zertifizierungssystemen, die auf die Verarbeitung von Beschäftigtendaten und dringliche Probleme im Beschäftigungskontext ausgerichtet sind, in Erwägung gezogen werden. An der Ausarbeitung solcher Zertifizierungssysteme müssten die entsprechenden Interessengruppen, also Arbeitnehmer*innen und ihre Vertretungen, beteiligt werden.

3

ÜBERPRÜFUNG VON ALGORITHMEN IN UNABHÄNGIGEN UNTERSUCHUNGEN

In den vergangenen Jahren wurden diverse Methoden zur Überprüfung algorithmischer Systeme ausprobiert, vor allem bei Unternehmen, die nicht gewillt oder in der Lage sind, deren Auswirkungen auf die Arbeitsbedingungen offen darzulegen. Diese Untersuchungsmethoden können datenschutzrelevante und arbeitsrechtliche Verstöße aufdecken. Die dadurch erlangten Beweise könnten verwendet werden, um strategische Rechtsverfahren einzuleiten oder zu unterstützen, sie können als Druckmittel in Kollektivverhandlungen dienen oder zur Sensibilisierung der Arbeitnehmer*innen und der allgemeinen Öffentlichkeit herangezogen werden.

Diese Methoden wurden von neuartigen Organisationen wie Worker Info Exchange, PersonalData.io, Reversing.Works und dem Workers' Algorithm Observatory entwickelt und getestet. Alle bislang entwickelten Methoden erfordern die Einwilligung und Mitwirkung der Beschäftigten, um die benötigten Daten für weiterführende Analysen zu erheben. Die wichtigsten Datenerhebungsmethoden sind:

- **Zugriffsanfragen von Datensubjekten (Data Subject Access Requests, DSAR):** Arbeitnehmer*innen können ihre Datenrechte gemäß DSGVO geltend machen und eine Kopie ihrer eigenen Daten anfordern. Dazu können sie eine E-Mail an das Unternehmen senden oder eine dritte Partei damit beauftragen, dies in ihrem Namen zu erledigen. Der Nachteil dieser Vorgehensweise ist, dass Unternehmen ihnen unter Umständen unvollständige oder unverständliche Daten senden – oder einfach überhaupt nicht reagieren. Eine ausbleibende Antwort ist an sich ein Verstoß gegen die DSGVO und stellt kein unüberwindbares Hindernis dar – die Datenschutzbehörden können eingreifen und Unternehmen anweisen, die geforderten Daten bereitzustellen –, macht diese Vorgehensweise aber komplizierter und kostspieliger.

- ***Data Scraping* (Datenextraktion):** Bei anderen Methoden der Datenerhebung von einzelnen Arbeitskräften machen diese regelmäßig Screenshots von ihrer beruflichen App oder ermächtigen eine Software, dies für sie zu tun. Aber wie auch bei den DSAR erfordert diese Methode in der Regel die Mitwirkung einer recht großen Anzahl an Arbeitskräften.

- **Black-Box-Analyse:** Bei dieser Methode muss eine Arbeitskraft ihren Login und ihr Passwort an eine/n Techniksachverständige/n weitergeben, der/die sich daraufhin in die App einloggen und analysieren kann, welche Daten erhoben und an die Plattform oder andere Unternehmen weitergegeben werden. Bei dieser Methode reicht schon die Mitwirkung einer einzelnen Arbeitskraft aus, um nützliche Ergebnisse hervorzubringen.

Die Wirksamkeit dieser Methoden hängt davon ab, ob die Ergebnisse mit einer großen Anzahl an Mitwirkenden und über einen längeren Zeitraum reproduziert werden können. Die so erhobenen Daten können Elemente der im algorithmischen System eingebetteten Logik nachweisen, reichen aber womöglich nicht aus, um für ein vollständiges Bild zu sorgen. Forscher*innen und Fachleute aus der Praxis mit technischen, rechtlichen und sozialen Fachkenntnissen haben organisations- und länderübergreifend zusammen Methoden entwickelt, getestet und kombiniert, die weiterführende unabhängige Überprüfungen von algorithmischen Systemen ermöglichen.

Als größte Herausforderung stellte sich dabei eine engere Zusammenarbeit mit den Arbeitnehmerorganisationen heraus, die dazu beitragen können, weitere Verletzungen der Privatsphäre und Verstöße gegen das Arbeitsrecht zu ermitteln. Gewerkschaften und Arbeitnehmerorganisationen können dabei helfen, indem sie technische Untersuchungen mit den Beanstandungen von Arbeitnehmer*innen verbinden. Außerdem können sie die Ergebnisse ihrer technischen Untersuchungen in ihren kollektiven Bemühungen zur Verbesserung der Arbeitsbedingungen einsetzen.

Bei den bisherigen unabhängigen technischen Überprüfungen ging es vor allem um Plattformarbeit, insbesondere im Liefer- und Transportsektor. Zukünftige Überprüfungen könnten auch Datenverarbeitungssysteme und -praktiken an »traditionellen« Arbeitsplätzen ins Visier nehmen.

4

MEHR RECHTLICHE KLARHEIT UND BESSERE KONFORMITÄT DURCH STRATEGISCHE RECHTSVERFAHREN

Angesichts der unzureichenden beschäftigungsspezifischen Datenschutznormen und der erheblichen Defizite bei ihrer Einhaltung befassten sich die Workshop-Teilnehmer*innen damit, welches Potenzial »strategische Rechtsverfahren« zur Klarstellung und Durchsetzung der DSGVO-Bestimmungen haben. Strategische Rechtsverfahren sind in der Regel Gerichtsprozesse, aber im Zusammenhang mit Datenschutzgesetzen können auch die Datenschutzbehörden eine wichtige Rolle übernehmen.

Arbeitnehmer*innen und ihre Vertretungen müssen beim Einreichen einer Beschwerde bei einer Datenschutzbehörde vor allem weniger Schwierigkeiten bewältigen als bei einem Gerichtsverfahren, da eine Beschwerde nicht mit ausführlichen juristischen Argumenten einhergehen muss, sofern sie überzeugende Beweise für die potenziellen DSGVO-Verstöße enthält. Als Beweis käme zum Beispiel eine Kopie des E-Mail-Verkehrs mit dem Unternehmen infrage, aus dem hervorgeht, dass das Unternehmen der Zugriffsanfrage des Datensubjekts (DSAR) nicht vollständig nachgekommen ist. Auch Bilder oder Screenshots der als problematisch angesehenen Software und ihrer Funktionen sind denkbar.

Eine ausführlichere Dokumentation der technischen Überprüfung inklusive Analysen der Daten aus mehreren DSAR, Datenextraktionen oder Black-Box-Analysen kann ebenfalls zur Untermauerung der Beschwerde bei der Behörde vorgelegt werden, ist aber nicht nötig. Im Idealfall hat eine fundierte Beschwerde zur Folge, dass eine Datenschutzbehörde eigene Untersuchungen der Vorgehensweisen eines Unternehmens in die Wege leitet. Derartige Untersuchungen können auf verschiedene Sanktionen hinauslaufen. Das Unternehmen kann zum Beispiel zu Abhilfemaßnahmen gezwungen werden, oder ihm wird eine empfindliche Geldbuße auferlegt, die für andere Firmen als Abschreckung dienen soll.

Die Zivilgesellschaft kann dazu beitragen, indem sie Akteur*innen beim Sammeln von Beweisen für Verstöße und deren Einreichung bei nationalen Datenschutzbehörden oder Arbeitsgerichten im Zuge von Beschwerden unterstützt. Ziel ist es, Rechts- und Behördenentscheidungen herbeizuführen, die die Rechtssicherheit verbessern; Arbeitnehmer*innen, Gewerkschaften, Arbeitgeber*innen, Softwareanbieter*innen und Behörden für die Regeln zu sensibilisieren; und Unternehmen durch Geldbußen Anreize zur Konformität zu setzen. Eine solche Strategie der Unterstützung der Akteur*innen »von unten« kann vor allem zur Präzisierung von Vorschriften auf nationaler Ebene hilfreich sein, da Arbeitnehmer*innen und Gewerkschaften befürchten könnten, dass die privatrechtliche Durchsetzung durch Rechtsverfahren zeitaufwendig ist und hohe Kosten für Rechtsexpert*innen anfallen könnten. Vor allem die Einführung einer Plattform zum Austausch von Methoden zum Sammeln und Analysieren von Beweisen, aber auch von Erfahrungen und Fachkenntnissen wäre eine Überlegung wert.

Aber auch ein »Top-Down-Ansatz« wie der, für den die Datenschutzorganisationen »None of Your Business« (NOYB) und Foxglove die Vorarbeit geleistet haben, wäre denkbar. Diese Organisationen haben ihr Hauptaugenmerk zwar nicht auf Arbeitnehmer*innen als spezielle Kategorie von Datensubjekten gerichtet, eventuell haben sie aber Interesse daran, ihre Aufgabenbereiche auf Beschäftigte auszuweiten. Man könnte auch eine neue Organisation gründen, die sich ausschließlich mit Arbeitnehmer*innen als Datensubjekte befasst. Wie bereits in Abschnitt 2.2 festgehalten wurde, sollte weiter erforscht werden, in welchen Ländern solche Organisationen angesichts der zwischen den EU-Mitgliedstaaten stark variierenden nationalen Vorschriften für kollektive Ansprüche die Arbeitskräfte gemäß Art. 80 Abs. 2 vertreten könnten. Eine solche Organisation wäre bestens aufgestellt, um rechtliche Strategien auf EU-Ebene zu erkunden und Gerichtsverfahren anzustrengen, die möglicherweise bis vor den Europäischen Gerichtshof (EuGH) gehen.

5

DIE NÄCHSTEN SCHRITTE FÜR SOZIALPARTNER, DIE FORSCHUNG UND DIE ZIVILGESELLSCHAFT

In den vorhergehenden Abschnitten ging es um diverse, bislang nicht voll ausgeschöpfte Optionen zur Verbesserung der DSGVO-Konformität im Beschäftigungskontext. Diese Optionen würden aber natürlich auch stark von einer besseren Durchsetzung durch die Datenschutzbehörden profitieren. Daher wäre eine Ausweitung der Kapazitäten und Aktivitäten von Datenschutzbehörden vor allem im Bereich der Verarbeitung von Beschäftigtendaten äußerst begrüßenswert. Dafür wären verschiedenen Wissenschaftler*innen (Nogarede 2021, ICCL 2021, 2023; NOYB 2022, 2023) zufolge auch eine ausreichende Finanzausstattung der Behörden und Investitionen in technische Fachkenntnisse sowie eine bessere effektive Durchsetzung und partnerschaftliche Zusammenarbeit nötig.

Vor diesem allgemeinen Hintergrund werden in diesem Abschnitt die nächsten Schritte für die konkreten, in den Abschnitten 2, 3 und 4 dargelegten Bereiche erörtert, um die Umsetzungslücken beim Datenschutz im Beschäftigungskontext zu schließen.

5.1 DATENSCHUTZGESETZE KLARSTELLEN, SPEZIFIZIEREN UND AUSSCHÖPFEN

Wie bereits erwähnt, wird die Einhaltung der Datenschutzvorschriften im Arbeitsumfeld dadurch erschwert, dass keiner der Mechanismen zur Anpassung der DSGVO an den Beschäftigungskontext – weder Gesetze gemäß Art. 88 noch Kollektivvereinbarungen, Zertifizierungssysteme oder Verhaltensregeln – ausreichend ausgenutzt wird.

GESETZE UND KOLLEKTIVVERHANDLUNGEN

In der hiermit einhergehenden Publikation »Stärkung der Datenschutzrechte von Arbeitnehmer*innen« zeigt Halefom Abraha den Gewerkschaften auf, wie sie die Datenschutzgesetze für das Arbeitsumfeld konkretisieren können. Dies kann als Muster für Gesetze und Kollektivvereinbarungen gemäß Art. 88 zur Anwendung in ganz Europa genutzt werden.

Die Zivilgesellschaft und Arbeitnehmerorganisationen können diese Abhandlung und die zugrundeliegenden Prinzipien nutzen, um Gespräche mit den jeweiligen Regierungen und zwischen den Sozialpartnern in die Wege zu leiten. Wenn die deutsche Regierung ihre Ankündigung im Zuge der Datenstrategie 2023 (*Fortschritt durch Datennutzung*), mit der sie ihren Entwurf für das Beschäftigtendatenschutzgesetz veröffentlichte, umsetzt, kann sie neue Impulse setzen.

VERHALTENSREGELN UND ZERTIFIZIERUNGEN

In der Praxis erweist es sich als schwierig, die Datenschutzrechte der Beschäftigten zu wahren. Gleichzeitig herrscht bei Unternehmen aller Größenordnungen Unsicherheit darüber, wie die DSGVO im Beschäftigungskontext umzusetzen ist. Viele Anforderungen aus der DSGVO könnten in Verhaltensregeln und Zertifizierungssystemen präzisiert werden. Eine der Bestimmungen, die von einer solchen Präzisierung profitieren würde, ist der Art. 25 DSGVO, der vorsieht, dass Datenverantwortliche »geeignete technische und organisatorische Maßnahmen« treffen, um den »Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen« zu gewährleisten.

Für den Anfang könnten zukünftige Forschungen bewerten, inwiefern die gebräuchlichen Arbeitssoftwaresysteme die Anforderungen aus Art. 25 erfüllen, und wenn nicht, welche technischen und organisatorischen Veränderungen vorgenommen werden könnten, um die Konformität zu verbessern. Da festgestellt wurde, dass sogar die Europäische Kommission selbst durch ihre Nutzung des Softwarepakets »Microsoft 365« die Datenschutzregeln verletzt (EDSB 2024, wäre dies ein besonders relevanter Fall, den es zu berücksichtigen gilt. Eine solche Bewertung könnte auch klären, welche Elemente sich für Verhaltensregeln und Zertifizierungssysteme eignen, und ihre Notwendigkeit untermauern.

Neben der Bewertung der Konformität einzelner Softwarepakete mit der DSGVO könnten sich die Akteur*innen der Zivilgesellschaft auch mit der Präzisierung der Gesetze durch Verhaltensregeln und Zertifizierungssysteme befassen. Dazu könnten zunächst Interviews und Workshops zu diesen Regeln und Systemen für Arbeitgeber*innen, die personenbezogene Beschäftigtendaten mit Software verarbeiten, unter Einbeziehung der jeweiligen Interessengruppen – in erster Linie Arbeitgeber- und Arbeitnehmervertre-

tungen, aber auch mit Softwareanbieter*innen – durchgeführt werden. Diese Forschungen könnten nicht nur potenzielle Inhalte dieser Regeln, sondern auch mögliche Prozesse zur Absicherung der kontinuierlichen Einbeziehung von Arbeitnehmer*innen in ihre Ausarbeitung, Durchsetzung und Weiterentwicklung erkunden.

Zu den Vor- und Nachteilen jeder Option in einem bestimmten Arbeitskontext müssen weitere Untersuchungen durchgeführt werden. Zwar sind sowohl Verhaltensregeln als auch Zertifizierungssysteme freiwillig, aber bei Zertifizierungssystemen gemäß DSGVO gibt es keine Vorgaben, wer die Kriterien ausarbeiten darf. Die Gestaltung von Verhaltensregeln hingegen ist »Verbänden und andere[n] Vereinigungen, die [...] Verantwortliche oder Auftragsverarbeiter vertreten«, vorbehalten. Abgesehen davon müssten Zertifizierungssysteme wahrscheinlich von nationalen Zertifizierungsstellen verwendet werden, um gültig zu sein.

Zivilgesellschaftliche Forschungen könnten also Vertreter*innen von möglicherweise relevanten Organisationen (wie regionalen und nationalen Datenschutzbehörden), technischen Prüfverbänden (wie TÜV) und Akkreditierungsstellen (wie DakkS oder ILNAS) in Sondierungsgespräche einbeziehen, um ihre möglichen Rollen bei der Ausarbeitung dieser Mechanismen und Unterstützung ihrer Anwendung zu erörtern.

5.2 STÄRKERE PRIVATRECHTLICHE DURCHSETZUNG VON DATENSCHUTZGESETZEN

Wie eingangs erwähnt, lässt die Einhaltung der Datenschutzgesetze im Beschäftigungskontext stark zu wünschen übrig. Zwar werden neue Verfahrensregeln zur Verbesserung der Zusammenarbeit zwischen den Datenschutzbehörden ausgehandelt, aber diese sind allein vermutlich nicht in der Lage, etwas an der Situation zu ändern. Darüber hinaus werden die Datenschutzbehörden aufgrund der kürzlich verabschiedeten Richtlinie zur Plattformarbeit und dem AI Act in Zukunft vor noch größeren Verpflichtungen und Koordinationsproblemen stehen. Vor diesem Hintergrund geht es in diesem Abschnitt um die nächsten Schritte, die Arbeits- und andere Organisationen der Zivilgesellschaft unternehmen können, um die Einhaltung und Durchsetzung von Datenschutzvorschriften am Arbeitsplatz voranzubringen.

BEWEISE SAMMELN

Berichten zufolge wird die DSGVO an den wenigsten Arbeitsplätzen wirklich eingehalten. Aber das weiß, abgesehen von Expert*innen und Fachleuten aus der Praxis, kaum jemand. Eine wirksame Maßnahme für Arbeitnehmerorganisationen und andere Akteur*innen der Zivilgesellschaft bestünde deshalb darin, offensichtliche und geläufige DSGVO-Verstöße im Arbeitsumfeld aufzulisten – entweder in einem kurzen Bericht oder besser noch in einer Online-Datenbank. Diese könnte ergänzt werden durch Umfragen, Fokusgruppen oder andere Methoden, um die Einstellung der Arbeitnehmer*innen zu den DSGVO-Rechten zu verstehen, und um einen besseren Überblick über die Nichteinhaltung zu erlangen, zum Beispiel im Hinblick auf die in Art. 13 und 14 DSGVO dargelegten Informationsrechte. Durch diese Maßnahmen würde auch die Allgemeinheit erfahren, was die Expert*innen schon länger wissen, und dazu beitragen, die Nichteinhaltung auf die politische Agenda zu setzen. Sozialpartner, Wissenschaftler*innen und die Zivilgesellschaft könnten dadurch ihre Bemühungen konkretisieren.

ARBEITNEHMERVERTRETUNGEN ZUR ZUSAMMENARBEIT MIT TECHNIKEXPERT*INNEN ANREGEN

Manche Nachweise können nur mit technischen Fachkenntnissen erlangt werden. Daher wurden in Abschnitt 3 technische Methoden zur Offenlegung von datenschutzrelevanten und arbeitsrechtlichen Verstöße erläutert. Allerdings erweist es sich als schwierig, Technologieexpert*innen mit den Arbeitnehmervertretungen zusammenzubringen, die Beanstandungen der Arbeitnehmer*innen äußern und Rechtsverstöße ermitteln können.

Es wäre zu begrüßen, wenn die Arbeitnehmerorganisationen mehr Ressourcen für Datenschutz- und Data-Governance-Angelegenheiten einplanen, mehr Schulungen zu diesen Themen durchführen und ihre Bedeutung für Kollektivverhandlungen hervorheben. Einige Bemühungen in diese Richtung gibt es bereits (Colclough 2023). Sie könnten die derzeitigen Aktivitäten von Public Services International, FES »Zukunft der Arbeit« und UNI Europa und deren Online-Tools zum Sammeln von Informationen über bestehende Kollektivvereinbarungen, die auch die Datenerhebung am Arbeitsplatz beinhalten, ergänzen.

Zudem könnten die Arbeitnehmerorganisationen ihre Bemühungen verstärken, was die Aufnahme von Beziehungen mit – und leichtere Kontaktaufnahme zu – Technikexpert*innen wie Datenanalyst*innen betrifft. Angesichts des immer größer werdenden Gesetzeskorpus, der Arbeitnehmervertretungen die Konsultation externer Sachverständiger auf Kosten der Arbeitgeber*innen gestattet (deutsches Betriebsverfassungsgesetz § 80 Abs. 3; Richtlinie zur Plattformarbeit Art. 13 Abs. 3), bietet sich hier eine gute Gelegenheit.

STRATEGISCHE RECHTSVERFAHREN

Neben technischen Fachkenntnissen und dem Sammeln von Beweisen könnten Organisationen der Zivilgesellschaft auch helfen, reelle Möglichkeiten für strategische Rechtsverfahren im Zusammenhang mit Beschäftigtendaten zu ermitteln; dazu gehört auch das Einreichen von Beschwerden bei Datenschutzbehörden. Dazu müsste zunächst eine Rechtsanalyse durchgeführt werden, um herauszufinden, in welchen EU-Ländern Gewerkschaften »Initiativbe-

schwerden« gemäß Art. 80 Abs. 2 DSGVO oder anderen Gesetzen zu kollektiven Ansprüchen einreichen können, und welche Kosten, Risiken und Engpässe mit solchen Rechtsverfahren einhergehen.

Hilfreich wäre auch eine Auflistung der vorhandenen Interessengruppen, die sich für die Verbesserung der Datenschutzrechte von Arbeitnehmer*innen einsetzen, um herauszufinden, ob sie durch Verwaltungs- und Rechtsverfahren zu einem besseren Datenschutz am Arbeitsplatz beitragen können, oder ob es sich lohnt, eine neue Organisation zu gründen, die sich ausschließlich mit den Rechten von Arbeitnehmer*innen als Datensubjekten befasst. Eine solche Organisation wäre vielleicht besser in der Lage, rechtliche Strategien auf EU-Ebene zu erkunden und Gerichtsverfahren anzustrengen, die möglicherweise bis vor den Europäischen Gerichtshof (EuGH) gehen.

REFERENZEN

Abraha, H. (2022). A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. *International Data Privacy Law* 12(4) 276–296. https://doi.org/10.1093/idpl/ipac015.

Abraha, H. (2023). Hauptpersonalrat der Lehrerinnen und Lehrer: Article 88 GDPR and the Interplace between EU and Member State Employee Data Protection Rules. *The Modern Law Review* 87(2) 484-496. https://doi.org/10.1111/1468-2230.12849.

Abraha, H. (2024). *Stärkung der Datenschutzrechte von Arbeitnehmer*innen*. Friedrich-Ebert-Stiftung, Juni.

Adams, Z. und Wenckebach, J. (2023). Collective regulation of algorithmic management. *European Labour Law Journal* 14(2): 211–229. https://doi.org/10.1177/20319525231167477.

BEUC (2023). Recommendations on harmonising procedural matters in the GDPR, März. Aufgerufen unter: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-034_recommendations_on_harmonising_cross-border_procedural_matters_in_the_GDPR.pdf.

Bundesregierung (2023). Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung, August. Aufgerufen unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.html.

Calacci, D. und Stein, J. (2023). From access to understanding: Collective data governance for workers. *European Labour Law Journal* 14(2): 253–282. https://doi.org/10.1177/20319525231167981.

Cefaliello, A., Moore, P. V. und Donoghue, R. (2023). Making algorithmic management safe and healthy for workers: Addressing psychosocial risks in new legal provisions. *European Labour Law Journal* 14(2) 192–210.

Christl, W. (2021). Digitale Überwachung und Kontrolle am Arbeitsplatz: Von der Ausweitung betrieblicher Datenerfassung zum algorithmischen Management? Wien: Cracked Labs/Arbeiterkammer Wien. https://crackedlabs.org/dl/CrackedLabs_Christl_UeberwachungKontrolleArbeitsplatz.pdf.

Christl, W. (2023). Monitoring, Streamlining and Reorganizing Work with Digital Technology: A case study on software for process mining, workflow automation, algorithmic management and AI based on rich behavioral data about workers. Wien: Cracked Labs/Arbeiterkammer Wien. https://crackedlabs.org/dl/CrackedLabs_Christl_Celonis.pdf.

Colclough, C. (2023). Protecting workers´ rights in digitised workplaces. *Equal Times*, 4. Mai. Aufgerufen unter: https://www.thewhynotlab.com/publications/protecting-workers-rights-in-digitised-workplaces.

Dewitte, P. (2023). A Brief History of Data Protection by Design. From multilateral security to Article 25(1) GDPR. *Technology and Regulation* 80–94. https://doi.org/10.26116/techreg.2023.008.

Europäischer Datenschutzausschuss (EDSA) (2020). Leitlinien 4/2019 zu Artikel 25. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Version 2.0. Aufgerufen unter: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

Europäischer Datenschutzbeauftragter (EDSB) (2024). European Commission´s use of Microsoft 365 infringes data protection law for EU institutions and bodies, March. Pressemitteilung. Aufgerufen unter: https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf.

Irish Council for Civil Liberties (ICCL) (2021). Europe´s enforcement paralysis. Aufgerufen unter: https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf.

Irish Council for Civil Liberties (ICCL) (2023). 5 years: GDPR´s crisis point. Aufgerufen unter: https://www.iccl.ie/digital-data/iccl-2023-gdpr-report/.

Kamara, I. und De Hert, P. (2018). Data Protection Certification in the EU: Possibilities, Actors and Building Blocks in a reformed landscape, 7–33. In Rodrigues, R. und Papakonstantinou, V. (Hrsg.). *Privacy and Data Protection Seals*. T.M.C. Asser Press.

Nogarede, J. (2021). Keine Digitalisierung ohne Vertretung. Eine Analyse politischer Initiativen für mehr Mitbestimmung der Arbeitnehmer*innen in der digitalen Arbeitswelt. Politische Studie der FEPS, November. Aufgerufen unter: https://feps-europe.eu/publication/826-no-digitalisation-without-representation/.

NOYB (2022). Annual Report 2022. Aufgerufen unter: https://noyb.eu/en/annual-report-2022-out-now.

NOYB (2023). 5 Years of the GDPR: National Authorities let down European Legislator, Mai. Aufgerufen unter: https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator.

Pato, A (2019). The national adaptation of article 80 GDPR: Towards the effective private enforcement of collective data protection rights, 98–106. In: McCullagh, K., Tambou, O. und Bourton, S. (Hrsg.). National Adaptations of the GDPR, Collection Open Access Book, Blogdroiteuropeen, Luxemburg, Februar 2019.

Silberman, M. und Johnston, H. (2020). Using GDPR to improve legal clarity and working conditions on digital labour platforms. Arbeitspapier 2020.05. ETUI. Aufgerufen unter: https://www.etui.org/sites/default/files/2020-06/WP%202020.05%20GDPR%20Working%20conditions%20digital%20labour%20platforms%20Silberman%20Johnston%20web.pdf.

Von Grafenstein, M. (2021). Specific GDPR certification schemes as rule, general schemes (and criteria) as exception. HIIG Discussion Paper 2021-04. DOI 10.5281/zenodo.4905484.

ÜBER DIE AUTOR:INNEN

Justin Nogarede ist leitender Fachreferent am FES-Kompetenzzentrum »Zukunft der Arbeit«. Seine Themenschwerpunkte sind Datenschutz im Beschäftigungskontext und die politische Ökonomie der Digitalisierung. Zuvor war er Analyst für Digitalpolitik bei der Foundation for European Progressive Studies (FEPS). Außerdem war er im Generalsekretariat der Europäischen Kommission unter anderem für bessere Regulierung, Anwendung von EU-Recht und diverse politische Strategien im Bereich digitale Märkte und Binnenmarkt zuständig.

Michael ›Six‹ Silberman ist Postdoktorand im »iManage«-Projekt zum Thema „Rethinking Employment Law for a World of Algorithmic Management" am Bonavero Institute of Human Rights der Universität Oxford. Außerdem ist er Dozent für soziotechnische Systeme am London College of Political Technology (Newspeak House). Zuvor war er für die IG Metall tätig und befasste sich dabei vor allem mit den Rechten von Arbeitskräften von digitalen Arbeitsplattformen.

Joanna Bronowicka ist Soziologin am Center for Interdisciplinary Labour Law Studies der Europa-Universität Viadrina Fankfurt (Oder). Dort erforscht sie algorithmisches Management, Resistenzmethoden und die Mobilisierung von Plattformarbeitskräften in Berlin. Zuvor leitete sie das Zentrum für Internet und Menschenrechte und war als Analystin für das polnische Ministerium für Digitalisierung tätig.

Danksagungen

Unser besonderer Dank gilt Christina Colclough für ihre Unterstützung bei dem Workshop im Oktober 2023 und ihre Mitwirkung an diesem Bericht sowie den Teilnehmer*innen des Workshops für ihre Zeit und Einblicke. Wir danke James Turner für die Redaktion dieses Berichts und Ha-Thu Mai vom FES-Kompetenzzentrum »Zukunft der Arbeit« für die Mitorganisation des Workshops. Die Mitwirkung und der Zeitaufwand von Co-Autor Michael ›Six‹ Silberman wurden teilweise 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 978-3-98628-672-9