

Impulse für die Implementierung der Plattformarbeiterrichtlinie

Hintergrund

Lieferando wurde bereits 2009 in Berlin gegründet und hat die rasante Entwicklung der On-Demand-Lieferbranche aus erster Hand miterlebt. Auf Basis dieser langjährigen Erfahrungen setzt sich Lieferando für einen **einheitlichen, ausgewogenen und zukunftsorientierten Regulierungsansatz** der Plattformarbeit ein. Ziel ist es, ein Gleichgewicht zwischen **fairen Arbeitsbedingungen für Kurierere** und einem **tragfähigen, flexiblen Liefermodell** zu schaffen, das den Bedürfnissen von Kurieren, Handelspartnern und Kunden entspricht. Nur durch einen für die Branche geeigneten Rechtsrahmen können Schutz und sichere Arbeitsplätze für Kurierere gewährleistet und gleichzeitig eine wirtschaftlich tragfähige und skalierbare Geschäftstätigkeit ermöglicht werden.

Ursprünglich wurden alle über Lieferando bestellten Speisen entweder vom Kunden abgeholt oder direkt vom Restaurant selbst geliefert. Noch heute wird der Großteil unserer Bestellungen nicht von oder über Lieferando ausgeliefert, obwohl wir seit dem Jahr 2016 über die Takeaway Express B.V. & Co. KG (ebenfalls Teil der Just Eat Takeaway Group) mit vielen Tausend angestellten Kurieren eine Lieferung für Partner ohne eigene Fahrer anbieten.

Die **EU-Plattformarbeiterrichtlinie** lässt den Mitgliedstaaten für die Regulierung der Beschäftigungsvermutung und der Subunternehmerkontrolle bewusst Spielraum, um diese an die lokalen Gegebenheiten anzupassen. Zudem bereitet der **EU Quality Jobs Act** aktuell einheitliche Standards für Nachunternehmer vor. Damit die Plattformarbeiterrichtlinie nicht zu einem weiteren Standortnachteil für Deutschland wird, sind Beschäftigungsvermutung und Nachunternehmerkontrolle so auszugestalten, dass sie Scheinselbstständigkeit bekämpfen, ohne legale Arbeitsmodelle unverhältnismäßig mit Bürokratie zu belasten. Die übrigen Maßnahmen zur Vereinheitlichung und Verbesserung der Arbeitsbedingungen sollten minimalinvasiv und rechtssicher umgesetzt werden, ohne dem von der Bundesregierung angestrebten Bürokratieabbau entgegenzustehen.

Forderungen

Eine wirksame Plattformarbeiterrichtlinie, die Arbeitnehmerrechte stärkt und Unternehmen nicht unverhältnismäßig belastet, braucht:

1. eine zielgerichtete und widerlegbare **Beschäftigungsvermutung** auf Basis der allgemeinen Prinzipien von Weisungsgebundenheit und Kontrollausübung mit Fokus auf den direkten Arbeitgeber (Kap. II),
2. eine wirksame und unbürokratische **Nachunternehmerkontrolle** durch ein Präqualifikationsverfahren, ein Zentralregister und eine kontrollabhängige Enthaltungsoption (Kap. I), dem EU Quality Jobs Act nicht vorweggreift,
3. eine verhältnismäßige und unbürokratische Umsetzung der Kap. III - V, harmonisiert mit bestehender und geplanter Gesetzgebung zur Datennutzung in Unternehmen,
4. eine praxistaugliche Gestaltung der Nutzung von **Algorithmen**, um Rechtssicherheit bei Dokumentenkontrolle und Sicherheitsverfahren weiterhin zu ermöglichen (Kap. III Art. 7, 10 & 13).

Erläuterungen

1. Eine zielgerichtete und widerlegbare Beschäftigungsvermutung auf Basis der allgemeinen Prinzipien von Weisungsgebundenheit und Kontrollausübung mit Fokus auf den direkten Arbeitgeber (Kap. II)

In Deutschland wird der Beschäftigungsstatus hauptsächlich durch **§ 611a BGB** definiert, der sich auf die persönliche Abhängigkeit und das Weisungsrecht des Arbeitgebers bezüglich Inhalt, Ausführung, Zeit und Ort der Arbeit konzentriert. Dieser Rahmen legt fest, dass ein Arbeitnehmer an Weisungen gebunden und nicht wesentlich frei ist, seine Arbeit zu organisieren oder seine Arbeitszeiten zu bestimmen.

Für Zwecke der Sozialversicherung bietet **§ 7a SGB IV** ein sogenanntes **Statusfeststellungsverfahren** an, das zur Klärung des Beschäftigungsstatus eingeleitet werden kann, obwohl dieser Prozess oft langwierig und komplex ist und sowohl für Plattformen als auch für Arbeitnehmer Unsicherheit schafft.

Vorschlag zur Ausgestaltung der widerlegbaren Beschäftigungsvermutung

Hinsichtlich der widerlegbaren Beschäftigungsvermutung gemäß Artikel 5 empfehlen wir, auf starre, kriterienbasierte Schwellenwerte zu verzichten und stattdessen auf die allgemeine Auslegung von Weisungsgebundenheit und Kontrollausübung zu setzen. Eine Fokussierung auf die tatsächliche Ausübung von Kontrolle und die Weisungsgebundenheit ist rechtssicherer und verhindert, dass legitime Geschäftsmodelle durch formale Hürden unbeabsichtigt erfasst werden.

Zudem muss bei der Umsetzung klargestellt werden, dass die Beschäftigungsvermutung nicht zwangsläufig ein direktes Beschäftigungsverhältnis mit der Plattform begründet. Die Vermutung sollte primär gegen den direkten Arbeitgeber – im Falle von Intermediärmodellen also den Logistikpartner – gerichtet sein. Eine unmittelbare Haftung der Plattform sollte nur dann als ultima ratio eingreifen, wenn die Plattform selbst eine determinierende Kontrolle über die tatsächliche Ausübung der Tätigkeit des Arbeitnehmers ausübt. Dies entspricht dem Geist der Richtlinie, die kein generelles Verbot von Intermediärmodellen vorsieht, sondern den Schutz der Arbeitnehmer auf allen Ebenen gewährleisten will.

2. Wirksame und unbürokratische Nachunternehmerkontrolle durch ein Präqualifikationsverfahren und kontrollabhängige Enthaftungsoption (Kap. I Art. 3), dem EU Quality Jobs Act nicht vorweggreift.

Hinsichtlich der Nachunternehmerhaftung und -kontrolle umfasst der aktuelle Rechtsrahmen verschiedene Haftungsmodelle:

- § 14 AEntG (Arbeitnehmer-Entsendegesetz) mit einer umfassenden, verschuldensunabhängigen Haftung des Auftraggebers für Mindestlöhne ohne Freistellungsmöglichkeiten,
- § 28e Absätze 3a-3f SGB IV (Sozialgesetzbuch Viertes Buch) mit der Nachunternehmerhaftung für Sozialversicherungsbeiträge, die jedoch durch Unbedenklichkeitsbescheinigungen begrenzt werden kann, und
- § 13 MiLoG (Mindestlohngesetz) mit einer ebenso strikten verschuldensunabhängigen Haftung für Verstöße gegen den gesetzlichen Mindestlohn sowie das AEntG.

Die PWD lässt den Mitgliedstaaten die Flexibilität, die Einhaltung von Arbeitsstandards in der gesamten Lieferkette sicherzustellen. Das Ziel einer effektiven Nachunternehmerkontrolle muss darin bestehen, ein transparentes regulatorisches Ökosystem zu schaffen. Ein solcher Compliance-fokussierter Ansatz bietet verifizierten Drittanbietern Wettbewerbsvorteile, während er gleichzeitig Wettbewerber, die fragwürdige Praktiken anwenden, systematisch ausschließt und sie dazu zwingt, sich erhöhtem regulatorischen Druck und Haftungsrisiken zu stellen.

Vorschlag: Nationales Lizenzierungsverfahren mit kontrollabhängiger Haftungsfreistellung nach PSG-Vorbild

Wir schlagen die Einführung eines Präqualifikationsverfahrens vor, das sich am bewährten Modell des Paketboten-Schutz-Gesetzes (PSG) orientiert. Dieses Framework hat sich seit 2019 in der Paketlogistik als effektives Instrument zur Gewährleistung der Sozialversicherungs-Compliance bewährt und wurde aufgrund seiner Wirksamkeit 2025 erfolgreich ausgeweitet.

Dieser Ansatz umfasst folgende Kernpunkte:

- **Aktive Due-Diligence-Prüfung.** Wir bekennen uns zu einer aktiven und verantwortungsvollen Rolle bei der Durchführung strenger Vor-Onboarding-Audits. Bevor ein Nachunternehmer mit unserer Plattform interagieren darf, muss dieser ein rigides Prüfungsverfahren durchlaufen, das insbesondere die Überprüfung von Solvenz, steuerlicher Compliance sowie das Vorliegen aktueller sozialversicherungsrechtlicher Unbedenklichkeitsbescheinigungen umfasst.
- **Nationales Zertifizierungssystem.** Etablierung eines branchenspezifischen Registers für verifizierte Nachunternehmer. Der erfolgreiche Abschluss dieser Präqualifikation dient als Nachweis der Zuverlässigkeit und führt – analog zum PSG-Modell – zu einer Befreiung von der vollen Generalhaftung des Auftraggebers, während die operative Compliance-Verantwortung beim Nachunternehmer verbleibt.
- **Regulatorische Rechtssicherheit.** Durch die Anlehnung an das PSG-Modell schaffen wir einen verlässlichen Rechtsrahmen, der bereits seit Jahren erfolgreich praktiziert wird. Dies verhindert die Notwendigkeit von Experimenten mit unausgereiften Haftungsregeln und ermöglicht seriösen Unternehmen, durch konsequente Compliance Wettbewerbsvorteile zu generieren, während illegale Praktiken systematisch vom Markt verdrängt werden.

Dieser Ansatz schafft das notwendige Gleichgewicht zwischen dem regulatorischen Anspruch auf wirksame Kontrollen und der operativen Flexibilität für rechtskonforme Geschäftsmodelle.

3. Verhältnismäßige & unbürokratische Umsetzung der Kap. III - V, harmonisiert mit bestehender und geplanter Gesetzgebung zur Datennutzung in Unternehmen

Mehrere gleichzeitige Entwicklungen könnten die Umsetzung der PWD in Deutschland beeinflussen. Die Implementierung des KI-Gesetzes (AI Act) weist erhebliche Überschneidungen bei den Regelungen zum algorithmischen Management auf, die mit den Anforderungen der PWD harmonisiert werden müssen. Zusätzlich dazu ist eine Reform des Beschäftigtendatenschutzrechts geplant, die mit den Bestimmungen zur Datenverarbeitung in der Plattformarbeit interagieren wird. Auch die Erweiterung der Mitbestimmungsrechte des Betriebsrats bezüglich automatisierter Systeme nach dem Betriebsverfassungsgesetz (BetrVG) muss in Bezug auf die Anforderungen der PWD an algorithmisches Management und Transparenz berücksichtigt werden.

Vorschlag

Diese Initiativen müssen bei der PWD-Umsetzung berücksichtigt werden. Wenn eine Plattform bereits strenge Standards gemäß DSGVO (für Daten), DAC7 (für Berichterstattung) oder Mitbestimmungsrecht (für Konsultation) erfüllt, sollte dies als Erfüllung der entsprechenden PWD-Anforderung angesehen werden. Dieser Ansatz verhindert die Schaffung paralleler, doppelter Bürokratien und gewährleistet durch einen kohärenten Rechtsrahmen keine unnötigen Verwaltungsaufwände für konforme Plattformen.

4. Praxistaugliche Gestaltung der Nutzung von Algorithmen, um Rechtssicherheit bei Dokumentenkontrolle und Sicherheitsverfahren weiterhin zu ermöglichen (Kap. III Art. 7, 10 & 13)

Die Umsetzung von Kapitel III der PWD muss auf den betrieblichen Realitäten der digitalen Plattformarbeit basieren und den Grundsätzen der Sicherheit, der betrieblichen Durchführbarkeit und der Innovation entsprechen, das wirtschaftliche Überleben der Plattform nicht zu gefährden und keine widersprüchlichen rechtlichen Verpflichtungen zu schaffen.

Aktuell nutzt Lieferando **Algorithmen** im Arbeitsprozess nur für zwei Vorgänge: die effiziente Zuteilung von Bestellungen an Kuriere und die kilometergenaue Entschädigung für die Nutzung privater Fahrzeuge. Die Plattformarbeiterrichtlinie darf nicht dazu führen, dass Effizienzpotenziale durch technischen Fortschritt zukünftig nicht nutzbar sind. In der Natur der Plattformarbeit liegen eine hohe Fluktuation und eine dezentrale Arbeitsweise, die qua Geschäftsmodell auf die Nutzung und Verarbeitung von Daten angewiesen ist.

Kapitel III Art. 7 der Plattformarbeiterrichtlinie macht Vorgaben für die **Verarbeitung von personenbezogenen Daten ab Beginn des Einstellungsverfahrens**. Eine strenge, wörtliche Auslegung der PWD gefährdet unsere Fähigkeit, gesetzliche Verpflichtungen einzuhalten und unsere Nutzer zu schützen, was den Grundsätzen der Sicherheit und der betrieblichen Durchführbarkeit zuwiderläuft. Die Bedenken von Lieferando betreffen insbesondere die folgenden unbeabsichtigten Folgen:

- **Konflikt mit Sicherheit und Rechtskonformität (Art. 7, 10):** Strenge Verarbeitungsverbote bestimmter Datentypen (Art. 7) und die Anforderung einer menschlichen Überwachung für jede Sperrentscheidung (Art. 10) gefährden unsere Fähigkeit, Identitäten zu überprüfen, Betrug zu verhindern und sofortige Maßnahmen gegen akute Sicherheitsbedrohungen gegenüber unseren Kunden zu ergreifen. Automatisierte Systeme müssen in der Lage sein, binäre Entscheidungen auf der Grundlage objektiver Fakten (z. B. abgelaufene Dokumente/Arbeitserlaubnis) zu treffen und sofortige Präventivmaßnahmen (z. B. vorübergehende Kontosperrung bei fehlgeschlagener biometrischer Überprüfung oder Sicherheitsvorfall) ohne vorherige menschliche Intervention zu ergreifen, um die Einhaltung bestehender Gesetze (z. B. Verhinderung illegaler Arbeit) und die öffentliche Sicherheit zu gewährleisten.
- **Gefahr für Innovationen (Art. 7, 10, 13):** Die allgemeine Ausweitung der Beschränkungen durch Artikel 7 Absatz 3 auf automatisierte Systeme, die lediglich Entscheidungen unterstützen, und die Unklarheit hinsichtlich der Häufigkeit von Anfragen nach fachlicher Unterstützung (Art. 13) bergen die Gefahr, dass Ingenieurteams gelähmt werden und die Nutzung technischer Unterstützung für routinemäßige Verwaltungsaufgaben (z. B. Erinnerungen an das Ablaufdatum von Dokumenten) verhindert wird. Die PWD darf die Einführung technischer Fortschritte nicht behindern.
- **Störung der Personalbeschaffung (Art. 7 Abs. 2):** Die Anwendung von Beschränkungen ab Beginn des Einstellungsverfahrens führt zu einem unmöglichen Widerspruch, da Plattformen gesetzlich verpflichtet sind, die Identität und die Arbeitsberechtigung zu überprüfen, bevor eine Stelle angeboten werden kann. Automatisierte Überprüfungen müssen als Erfüllung einer gesetzlichen Verpflichtung zulässig sein.

Vorschläge

Wir sind überzeugt, dass eine **Differenzierung** zwischen automatisierter Unterstützung im Routinemanagement und der menschlichen Letztentscheidung sowie die klare Ausnahme für gesetzlich vorgeschriebene Sicherheits- und Rechtskonformitätsprüfungen eine ausgewogene und zukunftsfähige Implementierung der Plattformarbeiterrichtlinie in Deutschland ermöglichen. Ein zertifizierter Branchenstandard für den Umgang mit diesen Daten entsprechend Art. 7 Abs. 1 f) könnte gemeinschaftlich, unter enger Einbeziehung betrieblicher Realitäten und Notwendigkeiten, erarbeitet werden, ebenso wie die **Festlegung der Häufigkeit für Anfragen** nach Expertenunterstützung (**Art. 13**).

Siehe **Anhang A** für eine ausführlichere Stellungnahme zu den unbeabsichtigten Folgen von Kapitel III.

Der DSGVO Vorrang einräumen und Rechtssicherheit schaffen, insbesondere zwischen Art. 22 DSGVO und Art. 7 Abs. 3 PWD:

Kapitel III. Art. 7 der PWD ergänzt die DSGVO, welcher weiterhin der Vorrang eingeräumt werden muss - insbesondere hinsichtlich der Verantwortlichkeit für personenbezogene Daten sowie deren Definition. Das betrifft insbesondere Art. 22 DSGVO (das Recht, keiner Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die ihm gegenüber rechtliche Wirkung entfaltet oder ihn in ähnlicher Weise erheblich beeinträchtigt) und Art. 7 (3), der impliziert, dass der Artikel über automatisierte Überwachungssysteme und automatisierte Entscheidungssysteme hinausgeht, da er „Entscheidungen unterstützt, die Personen, die Plattformarbeit verrichten, in irgendeiner Weise betreffen“.

Klarstellung zur technischen Assistenz (Art. 7 Abs. 3):

Bei der nationalen Implementierung muss präzisiert werden, dass die Nutzung automatisierter Systeme zur **reinen technischen Unterstützung** von Routineaufgaben wie der Erkennung von Datenfeldern (z.B. Ablaufdaten) oder zur Erinnerungsfunktion für Dokumente, die **keine qualitative Bewertung** der Eignung oder Leistung der Person darstellen, nicht unter die Einschränkungen des Art. 7 Abs. 1 fallen.

Diese Assistenzsysteme dienen der Effizienz und Fehlervermeidung und ersetzen keine menschliche Entscheidung. Sie stellen keine Überwachung im Sinne der Richtlinie dar.

Ausnahme für die gesetzlich erforderliche Überprüfung von Identität und Arbeitserlaubnis (Art. 7 Abs. 1 f) und Art. 10:

Die nationale Umsetzung muss einen klar definierten **Ausnahmetatbestand** schaffen, der die zweckgebundene Verarbeitung personenbezogener und biometrischer Daten zur Erfüllung nationaler und europäischer Rechtsvorschriften explizit zulässt. Hierunter fallen mindestens die Identitätsüberprüfung bei der Einstellung und während der Plattformarbeit – einschließlich der Verhinderung illegaler Beschäftigung durch App-Sharing (z.B. mittels 1:1-Abgleich des Gesichts mit dem Ausweisdokument in der Datenbank) sowie die automatisierte Überprüfung von Arbeitserlaubnissen.

Definition des Einstellungs- und Auswahlverfahrens (Art. 7 Abs. 2):

Es muss klargestellt werden, dass die Beschränkungen für sensible Daten (Art. 7 Abs. 1 a-e) während des Einstellungsverfahrens gelten, die gesetzlich vorgeschriebenen Prüfungen der Identität und Arbeitserlaubnis jedoch als Erfüllung einer rechtlichen Pflicht stets zulässig sind, auch wenn sie biometrische Daten betreffen.

Die Notwendigkeit, unerwünschte oder nicht arbeitsberechtigte Personen frühzeitig vom Netzwerk fernzuhalten, dient der Sicherheit und der Integrität des Marktes.

Zusammenfassung

Um die Plattformarbeiterrichtlinie erfolgreich umzusetzen, ohne den deutschen Wirtschaftsstandort weiter zu benachteiligen, empfehlen wir eine 1:1-Umsetzung ohne Gold-Plating. Diese muss einerseits die Arbeitsbedingungen in der Plattformwirtschaft wirksam verbessern, andererseits aber unnötige bürokratische Hürden vermeiden oder dem EU Quality Jobs Act vorweggreifen. Es gilt, innovative Arbeitsmodelle zu ermöglichen und gleichzeitig einheitliche Wettbewerbsbedingungen zu gewährleisten, damit Deutschland als attraktiver Standort für Unternehmen und Arbeitnehmer gleichermaßen bestehen kann. Eine kluge Implementierung, die auf Praktikabilität und Rechtssicherheit setzt, ist hierfür von größter Bedeutung.

Head of Government Relations

Dr. Anna Dietrich
anna.dietrich@lieferando.de

Stand: Juli 2026

Unbeabsichtigte Folgen	Unterstützende Überlegungen, Gesetzgebung und praktische Beispiele	Lösung
Artikel 7: Beschränkungen der Verarbeitung personenbezogener Daten durch automatisierte Überwachungssysteme oder automatisierte Entscheidungssysteme		
Durch die Festlegung, dass die Verpflichtungen in diesem Artikel ab Beginn des Einstellungs- oder Auswahlverfahrens gelten (in Artikel 7.2), werden Arbeitsplattformen in der Erfüllung ihrer gesetzlichen Verpflichtungen, wie der digitalen Überprüfung der Identität, einer gültigen Arbeitserlaubnis oder eines Führerscheins, erheblich eingeschränkt. Durch die Festlegung, dass die Verpflichtungen in diesem Artikel auch für automatisierte Systeme gelten, die Entscheidungen unterstützen (Artikel 7.3), können Plattformen (effektiv) nicht a) Maßnahmen ergreifen gegen gemeldete Betrugsfälle, Aggressionen oder Straftaten sowie gegen diesbezügliche Beweise von Kunden oder Verbrauchern (wie schriftliche Mitteilungen oder Bildmaterial). b) Maßnahmen ergreifen gegen illegale Arbeit durch biometrische Kontrollen oder digitalen Betrug (DAC7), da digitale Kontrollen wie die Fotoüberprüfung möglicherweise verboten werden.	Erwägungsgrund 41: Die Durchführung einer biometrischen Überprüfung bleibt möglich, wenn die Identität durch den Abgleich der biometrischen Daten mit zuvor von derselben Person bereitgestellten Daten überprüft wird (Eins-zu-Eins-Überprüfung oder -Authentifizierung). Erwägungsgrund 59: Es ist von entscheidender Bedeutung, dass digitale Arbeitsplattformen eine zuverlässige Überprüfung der Identität der Personen gewährleisten, die Plattformarbeit verrichten. Es ist verboten, jemandem die Möglichkeit zu geben, ohne vorherige Überprüfung seiner Identität und seiner „Arbeitsberechtigung“ zu arbeiten. AML und DAC7: Unternehmen sind verpflichtet, kontinuierlich Verwaltungsdaten zur Verfügung zu stellen, um die Einhaltung der Steuer- und Finanzvorschriften zu gewährleisten. DSGVO (Artikel 6 Absatz 1 Buchstabe f – berechtigtes Interesse): Die Verarbeitung personenbezogener Daten, wie z. B. Korrespondenz oder Bildmaterial, das von Nutzern zur Meldung von Betrug, Aggression oder Straftaten bereitgestellt wird, basiert auf dem berechtigten Interesse der Plattform, die Sicherheit und Integrität ihrer Dienste für alle Nutzer zu gewährleisten. Diese Rechtsgrundlage ist unerlässlich, um die Verarbeitung für die Untersuchung von Vorfällen und die Einleitung von Maßnahmen zu ermöglichen, die andernfalls durch Artikel 7 Absatz 1 Buchstaben a und	Es sollte klargestellt werden, dass die in Artikel 7 festgelegten Beschränkungen der Datenverarbeitung die Verpflichtungen der digitalen Arbeitsplattform zur Einhaltung der EU- und nationalen Rechtsvorschriften unberührt lassen. Digitale Arbeitsplattformen dürfen nicht daran gehindert werden, personenbezogene Daten mittels automatisierter Überwachungssysteme oder automatisierter Entscheidungssysteme zu verarbeiten, wenn diese Verarbeitung erforderlich ist für: Einhaltung gesetzlicher Vorschriften: Die Überprüfung der Identität, der Arbeitsberechtigung und der beruflichen Qualifikationen (z. B. Führerscheine) gemäß den nationalen Einwanderungs-, Arbeits- und Straßenverkehrsgesetzen sowie Verpflichtungen in Bezug auf die Steuerberichterstattung (DAC7) und die Bekämpfung der Geldwäsche (AML). Sicherheit: Die Verarbeitung von Daten, einschließlich Kommunikations- und Standortdaten, wenn dies zur Verhinderung, Aufdeckung und Untersuchung von Sicherheitsvorfällen, Betrug oder kriminellen Aktivitäten gemäß den Bestimmungen der DSGVO zum berechtigten Interesse unbedingt erforderlich ist. Biometrische Überprüfung: Gemäß den Erwägungsgründen 41 und 59 der Richtlinie erstreckt sich das

	b eingeschränkt sein könnten. Plattformen müssen dieses Interesse gegen die Rechte der betroffenen Person abwägen, wobei jedoch der Schutz der öffentlichen Sicherheit und die Verhütung von Straftaten in der Regel Vorrang haben. Praxisbeispiel: Ein Plattformarbeiter versucht sich anzumelden. Das System fordert eine „Selfie-Überprüfung“ an, um zu verifizieren, dass es sich um den Kontoinhaber handelt (Betrugsbekämpfung). Dazu ist die Verarbeitung biometrischer Daten erforderlich. Wenn Artikel 7 Absatz 1 Buchstabe f als vollständiges Verbot ohne die in den Erwägungsgründen enthaltene Ausnahme für die Überprüfung ausgelegt wird, wird diese Sicherheitsüberprüfung rechtswidrig. Praxisbeispiel: Artikel 7 Absatz 1 Buchstabe c verbietet die Datenüberwachung außerhalb der aktiven Arbeitszeiten. Identitäts- und Dokumentenprüfungen finden häufig statt, wenn jemand nicht arbeitet (z. B. beim Hochladen eines neuen Reisepasses). Ohne automatisierte Kontrollen in diesen Momenten können Plattformen Identitätsbetrug und Geldwäsche nicht aufdecken. Darüber hinaus handelt es sich hierbei um gängige Systeme, die digitale Arbeitsplattformen ebenso wie nicht-digitale Arbeitsplattformen nutzen können sollten. Praxisbeispiel: Der Führerschein eines Plattformarbeiters läuft ab. Er lädt an einem Sonntag (während er nicht arbeitet) über die App einen neuen Führerschein hoch. Artikel 7 Absatz 1 Buchstabe c verbietet die Datenerhebung, wenn „keine Arbeit angeboten wird“. Eine strenge Auslegung würde eine digitale Arbeitsplattform zwingen, diese Compliance-Daten abzulehnen, bis der Plattformarbeiter „im Dienst“ ist. Praxisbeispiel: Bei jedem	Verbot biometrischer Daten nicht auf biometrische Überprüfungen, die ausschließlich zur Identitätsauthentifizierung und Betrugsbekämpfung verwendet werden.
--	---	--

	Auswahlverfahren sind die Bewerber gesetzlich verpflichtet, nachzuweisen, dass sie arbeitsberechtigt sind. Die Richtlinie schafft hier einen unmöglichen Widerspruch, da Daten gemäß Artikel 7 Absatz 1 Buchstabe c nur verarbeitet werden dürfen, wenn jemand Arbeit anbietet, aber Arbeit nur angeboten werden darf, wenn die Daten überprüft und somit verarbeitet wurden. Praxisbeispiel: Ein Plattformarbeiter wird wegen eines schweren Sicherheitsverstößes (z. B. Körperverletzung) während einer Lieferung angeklagt. Die digitale Arbeitsplattform muss zur Untersuchung auf Standortdaten zugreifen. Wenn die Beschränkungen gemäß Artikel 7 einen rückwirkenden Zugriff auf diese Daten verhindern, kann die digitale Arbeitsplattform ihrer Sorgfaltspflicht nicht nachkommen und nicht mit der Polizei zusammenarbeiten.	
Artikel 8: Datenschutz-Folgenabschätzung		
Artikel 8 der Richtlinie stuft automatisierte Überwachungs- und Entscheidungssysteme als „risikoreich“ ein und schreibt die Weitergabe von Datenschutz-Folgenabschätzungen (DPIAs) an Arbeitnehmervertreter vor. Eine unbeabsichtigte Folge einer strengen Auslegung ist die Verpflichtung zur Offenlegung vollständiger, ungeschwätzter technischer Audits. Dies würde digitale Arbeitsplattformen dazu zwingen, proprietären Quellcode, genaue algorithmische Gewichtungen (Geschäftsgeheimnisse) und spezifische Schwellenwerte für die Betrugsbekämpfung gegenüber externen Parteien offenzulegen. Dies schafft erhebliche Cybersicherheitsrisiken, erleichtert	Geschäftsgeheimnisse: DPIA enthalten sensible Informationen über die Funktionsweise von Algorithmen. Eine Offenlegung kann Plattformen anfällig für Manipulationen machen. Daher ist es wichtig, ein Gleichgewicht zwischen Transparenz, die den Plattformarbeitern hilft, einerseits und der operativen Durchführbarkeit und dem Schutz sensibler Informationen andererseits zu finden. Gemäß der Richtlinie 2016/943 haben digitale Arbeitsplattformen das Recht, Informationen in einer Weise weiterzugeben, die das geistige Eigentum und die Rechtsprivilegien schützt.	Die Verpflichtung, die Datenschutz-Folgenabschätzung den Vertretern der Personen, die Plattformarbeit verrichten, zur Verfügung zu stellen, ist so auszulegen, dass die Sicherheit und das geistige Eigentum der digitalen Arbeitsplattform gewahrt bleiben. Es sollte klargestellt werden, dass die Verpflichtung durch die Bereitstellung einer umfassenden, nicht technischen Zusammenfassung der Bewertung erfüllt ist. Diese Zusammenfassung muss die Logik des Systems, die verarbeiteten Daten und die Maßnahmen zur Minderung der Risiken für die Rechte und Freiheiten der Plattformarbeiter klar erläutern, ohne dass die vollständige technische Prüfung offengelegt werden muss. Es sollte klargestellt werden, dass

das „Ausnutzen“ des Systems durch böswillige Akteure und gefährdet das geistige Eigentum der Plattform, ohne einen Mehrwert für den Schutz der Datenrechte der Plattformarbeiter zu schaffen.		digitale Arbeitsplattformen die Meinung einer repräsentativen Stichprobe von Personen einholen sollten, die Plattformarbeit verrichten.
---	--	---

Artikel 9: Transparenz in Bezug auf automatisierte Überwachungssysteme und automatisierte Entscheidungssysteme

Die Definition von „Entscheidungen, die durch automatisierte Entscheidungssysteme unterstützt oder getroffen werden“ ist sehr weit gefasst. Dazu gehören auch einfache Tools (wie Excel-Tabellen), was zu unnötigen operativen Belastungen ohne Mehrwert für den Plattformarbeiter führt. Das Fehlen von Anforderungen an die Repräsentativität führt ebenfalls zu einer Fragmentierung. Plattformen müssen regelmäßig mit Parteien verhandeln, die kaum Arbeitnehmer vertreten, was den Dialog mit legitimen Vertretern erschwert.	Erwägungsgrund 39: Ein ausdrücklicher Fokus auf Systeme, die „erhebliche Auswirkungen“ auf die Beschäftigungsbedingungen haben. Eine Definition, die einfache Bürosoftware einbezieht, verfehlt dieses Ziel und schafft unnötige Belastungen. Praxisbeispiel: Wenn die genaue Gewichtung der Indikatoren in einem Betrugserkennungssystem veröffentlicht werden muss, werden Betrüger ihr Verhalten anpassen, um einer Entdeckung zu entgehen. Dies untergräbt die Integrität und Sicherheit der Plattform.	Es sollte klargestellt werden, dass sich die Transparenzpflichten in diesem Artikel auf automatisierte Systeme beziehen, die Entscheidungen mit erheblichen Auswirkungen auf die Arbeitsbedingungen, wie z. B. Auswirkungen auf die Bezahlung, treffen oder unterstützen. Systeme, die lediglich operative Geschäftsprozesse unterstützen und/oder nur administrative Aufgaben erfüllen und keinen wesentlichen Einfluss auf die Rechtsstellung des Plattformarbeiters haben, sollten von dieser Verpflichtung ausgenommen sein. Darüber hinaus sollte klargestellt werden, dass nur Entscheidungen, die aus automatisierten Entscheidungssystemen in den Anwendungsbereich fallen, resultieren, Darüber hinaus muss die Bereitstellung von Informationen verhältnismäßig sein und darf nicht zur Offenlegung von Geschäftsgeheimnissen führen, wie z. B. der genauen Funktionsweise dynamischer Preismodelle, die eine Manipulation des Systems ermöglichen könnten.
---	---	--

Artikel 10: Menschliche Aufsicht über automatisierte Überwachungssysteme und automatisierte Entscheidungsfindungssysteme

Die Anforderung, dass jede Entscheidung über eine Aussetzung von einem Menschen getroffen werden muss (Artikel 10 Absatz 5), gefährdet die öffentliche Sicherheit.	Erwägungsgrund 41: Die Durchführung einer biometrischen Überprüfung bleibt möglich, wenn die Identität durch den Abgleich der biometrischen Daten mit zuvor von derselben Person bereitgestellten Daten überprüft wird	Es sollte klargestellt werden, dass die in diesem Artikel festgelegten Beschränkungen nicht dazu dienen sollen, digitale Arbeitsplattformen daran zu hindern, durch biometrische Kontrollen wirksam gegen illegale Arbeit vorzugehen,
--	--	---

Dies führt zu Verzögerungen im Falle einer akuten Bedrohung, wie z. B. akuten Gewalttaten, und bei der Verhinderung von vorsätzlichem Identitätsbetrug und der Erleichterung der Arbeit. Bei binären Entscheidungen, die auf objektiven Fakten beruhen, wie z. B. einem abgelaufenen Führerschein oder einer abgelaufenen Arbeitserlaubnis, ist ein direktes menschliches Eingreifen nicht erforderlich.	(Eins-zu-Eins-Überprüfung oder Authentifizierung). Praxisbeispiel: Wenn eine biometrische Überprüfung während der Arbeit wiederholt fehlschlägt, ist es wünschenswert, dass die Person, die Plattformarbeit verrichtet, so schnell wie möglich Zugang zu einer menschlichen Überprüfung erhält. Damit kann der Verdacht auf illegale Arbeit bestätigt oder widerlegt werden (Artikel 10 Absatz 5). Es ist nicht wünschenswert, die Arbeit in der Zwischenzeit fortzusetzen, da jemand, der illegal arbeitet, kein Interesse daran hat, sich einer menschlichen Überprüfung zu unterziehen. Praxisbeispiel: Eine Plattform verarbeitet an einem Freitagabend 50 000 Bestellungen pro Stunde. Wenn Artikel 10 verlangt, dass ein Mensch diese Versandentscheidungen in Echtzeit „überwacht“ und validiert, um Fairness zu gewährleisten, würde der Dienst zusammenbrechen. Die Verzögerung würde das Essen und das Kundenerlebnis ruinieren.	wie in den Erwägungsgründen 41 und 59 sowie in den einschlägigen nationalen Rechtsvorschriften dargelegt. Gleiches gilt für akute Gewalttaten, die die öffentliche Sicherheit gefährden. Bei binären Entscheidungen, die auf eindeutigen Fakten beruhen, wie z. B. einem abgelaufenen Führerschein oder einer abgelaufenen Arbeitserlaubnis, ist ein direktes menschliches Eingreifen nicht erforderlich. Dies steht im Einklang mit den allgemein anerkannten Praktiken und Standards unter Arbeitgebern und Kunden. Beispiel: Es werden neue Geschäftsbedingungen eingeführt; wenn diese nicht vor einem bestimmten Datum akzeptiert werden, erlischt der Zugang zum System automatisch. Es sollte weiter geklärt werden, ob es ausreicht, dass ein Mensch ein Problem erkannt hat (die „menschliche Aufsicht“) und ein automatisiertes System eingerichtet hat (z. B. wenn ein Dokument abgelaufen ist, das Konto deaktivieren), und dass nach der Deaktivierung des Kontos keine weitere menschliche Aufsicht oder Überprüfung erforderlich ist.
Artikel 11: Menschliche Überprüfung		
Das Recht auf menschliche Überprüfung ist wichtig, aber ohne Schutzmaßnahmen anfällig für Missbrauch. Plattformen laufen Gefahr, automatisierte Massenanfragen zu erhalten, die zum Absturz des Systems führen können. Dies verlangsamt die Bearbeitung anderer Anfragen. Ein unbegrenztes Recht auf Überprüfung ohne Schwellenwerte für unbegründete oder wiederholte Anfragen	Praxisbeispiel: Ein Betrüger verwendet ein Skript, um Tausende von Überprüfungsanfragen zu stellen. Ohne die Möglichkeit, diese zu filtern, wird wertvolle Zeit für diesen „Spam“ aufgewendet, was zu Lasten anderer Plattformarbeiter geht, die relevante Anfragen stellen.	Stellen Sie klar, dass das Recht auf Überprüfung einer Entscheidung Schutz vor automatisierten Entscheidungen bieten soll, die rechtliche oder ähnlich bedeutende Auswirkungen auf den Plattformarbeiter haben (z. B. Suspendierung, Kündigung oder Nichtzahlung). Es erstreckt sich nicht auf routinemäßige operative Anweisungen, die für die Ausführung der Arbeit unerlässlich sind, wie z. B. die Zuweisung einzelner Aufgaben oder die Weiterleitung.

gefährdet die operative Durchführbarkeit.		Um einen Missbrauch dieses Rechts zu verhindern und die operative Durchführbarkeit für Plattformen sicherzustellen, müssen Überprüfungsanträge ausreichend begründet sein und dürfen nicht wiederholt oder schikanös sein. Werden Anträge von Vertretern von Personen gestellt, die Plattformarbeit verrichten, muss nachgewiesen werden, dass diese Vertreter von der Person, die sie zu vertreten vorgeben, dazu bevollmächtigt sind. Plattformen sind berechtigt, offensichtlich unbegründete oder übertriebene Anträge zu ignorieren.
---	--	---

Artikel 12: Sicherheit und Gesundheit

Artikel 12 Absatz 3 legt fest, dass digitale Arbeitsplattformen keine automatisierten Überwachungssysteme oder automatisierten Entscheidungssysteme in einer Weise einsetzen dürfen, die einen unangemessenen Druck auf Plattformarbeiter ausübt oder anderweitig die Sicherheit und die körperliche und geistige Gesundheit von Plattformarbeitern gefährdet. Es ist unklar, ob „unangemessener Druck“ positive Anreize wie Boni verbieten würde, bei denen Plattformarbeiter nach eigenem Ermessen entscheiden können, ob sie das kommerzielle Angebot annehmen oder nicht.	Praxisbeispiel: Um Plattformarbeiter zu ermutigen, effizient und unter Einhaltung der Sicherheits- und Verkehrsregeln zu arbeiten, hat JET Produktivitätsanreize auf der Grundlage der Anzahl der ausgelieferten Bestellungen eingeführt. Ein Bestellbonus wird auf der Grundlage der Anzahl der im Laufe eines Monats ausgelieferten Bestellungen berechnet. Um das Risiko für die Gesundheit und Sicherheit der Plattformarbeiter zu minimieren, werden bei der Berechnung des Bestellbonus nicht mehr als vier Lieferungen pro Stunde berücksichtigt. Daher werden Lieferungen, die über die dritte Lieferung innerhalb derselben Arbeitsstunde hinausgehen, bei der Berechnung des Auftragsbonus nicht berücksichtigt.	Es wird klargestellt, dass transparente Bewertungssysteme zur Qualitätsverbesserung und freiwillige Anreize nicht unter das Verbot in Artikel 12 Absatz 3 fallen.
---	--	--

Artikel 13: Unterrichtung und Anhörung

Artikel 13 führt die Verpflichtung für digitale Arbeitsplattformen ein, Arbeitnehmervertreter über Entscheidungen zu informieren und zu konsultieren, die zur Einführung oder zu „wesentlichen Änderungen“ bei der Verwendung automatisierter Überwachungs- oder	Praxisbeispiel: Eine digitale Arbeitsplattform aktualisiert ihre Routing-Engine, um einen neuen Kartenanbieter zu nutzen, der die Genauigkeit um 5 % verbessert. Dies ist eine technische Änderung. Wenn sie gemäß Artikel 13 als „wesentlich“ eingestuft wird, muss	Es sollte klargestellt werden, dass die Konsultationspflicht nur für Entscheidungen gilt, die wahrscheinlich zu einer wesentlichen und dauerhaften Änderung der Arbeitsbedingungen oder des Einkommens führen. Sie gilt nicht für:
---	--	---

Entscheidungssysteme führen können. Wenn „wesentliche Änderung“ zu weit ausgelegt wird (z. B. so, dass jede Softwareaktualisierung und jede Fehlerbehebung darunter fällt), wird dies die Innovationsfähigkeit einer digitalen Arbeitsplattform lähmen. Eine strenge Auslegung würde digitale Arbeitsplattformen dazu zwingen, notwendige technische Wartungsarbeiten oder Funktionsverbesserungen bis zum Abschluss der Konsultation auszusetzen, was die Benutzererfahrung und die Wettbewerbsfähigkeit beeinträchtigen würde. Darüber hinaus erlaubt Artikel 13 Absatz 3 den Vertretern, auf Kosten der digitalen Arbeitsplattform einen Sachverständigen zu benennen. Ohne Kostenobergrenzen oder strenge Vertraulichkeitsvorschriften besteht die Gefahr, dass eine Branche teurer „Algorithmus-Prüfer“ entsteht, die Zugang zu Geschäftsgeheimnissen erhalten, ohne einen Mehrwert für den sozialen Dialog zu schaffen.	die digitale Arbeitsplattform die Aktualisierung unterbrechen, Konsultationen einleiten und möglicherweise einen Experten für die Überprüfung der Kartendaten bezahlen. Die Einführung verzögert sich um drei Monate; in der Zwischenzeit leiden die Kuriere unter schlechten Routen. Praxisbeispiel: Ein Arbeitnehmersvertreter beantragt eine externe Prüfung für eine routinemäßige Aktualisierung des Bestellzuweisungsalgorithmus. Der ausgewählte Experte berechnet 500 € pro Stunde für eine 200-stündige Überprüfung. Wenn die digitale Arbeitsplattform diese Kosten nicht begrenzen oder die Notwendigkeit nicht anfechten kann, übersteigen die Compliance-Kosten den Wert der Softwareaktualisierung. Praxisbeispiel: Im Betrugserkennungssystem wird eine Schwachstelle entdeckt. Die Plattform muss diese sofort (innerhalb weniger Stunden) beheben. Wenn Artikel 13 eine „vorherige“ Konsultation für Änderungen an automatisierten Systemen vorschreibt, ist die Plattform rechtlich handlungsunfähig: Entweder sie behebt den Fehler und verstößt gegen die Richtlinie oder sie wartet auf die Konsultation und lässt das System angreifbar.	5. Routinemäßige Softwarewartung, Fehlerbehebungen oder Sicherheitspatches. 6. Geringfügige Anpassungen technischer Parameter (z. B. Kartenaktualisierungen, Optimierungen der Benutzeroberfläche), die die grundlegende Logik der Arbeitszuweisung oder Bezahlung nicht verändern. 7. Experimentelle Funktionen, die eine begrenzte Anzahl von Nutzern für einen begrenzten Zeitraum betreffen. Stellen Sie außerdem klar, dass digitale Arbeitsplattformen sofortige Änderungen ohne vorherige Konsultation vornehmen dürfen, wenn diese Änderungen unbedingt erforderlich sind, um Betrug zu verhindern, Sicherheitslücken zu beheben oder neuen gesetzlichen Verpflichtungen nachzukommen. Um einen Missbrauch des Rechts auf Unterstützung durch einen Sachverständigen gemäß Artikel 13 Absatz 3 zu verhindern, ist es von entscheidender Bedeutung, Schutzmaßnahmen wie eine gesetzliche Obergrenze oder eine angemessene Gebührenordnung für Sachverständigenhonorare, die Offenlegung von Interessenkonflikten vor der Ernennung und die Klarstellung, dass diese Sachverständigen kein uneingeschränktes Recht auf Zugang zum System haben, um beispielsweise den Quellcode oder andere wirtschaftlich sensible Informationen einzusehen, zu treffen.
---	---	---