Stellungnahme Beschäftigtendatenschutz

(Stand: 19.09.2023)

Bundesverband Deutsche Startups e.V.
Schiffbauerdamm 40
10117 Berlin
Tel.: +49 30 65 77 14 34
politik@startupverband.de
www.startupverband.de

Hintergrund

Das Bundesministerium für Arbeit und Soziales und das Bundesministerium des Inneren planen noch in der ersten Hälfte der 20. Legislaturperiode einen Entwurf für ein eigenständiges Gesetz zur Regelung des Beschäftigtendatenschutzes vorzulegen. Ziel des geplanten Gesetzes ist es, Beschäftigten und Arbeitgeber*innen durch klare und übersichtliche Vorschriften eine verlässliche Rechtsgrundlage für den Umgang mit Beschäftigtendaten zu bieten.

Laut einem Positionspapier der federführenden Ministerien bilden den Schwerpunkt des Gesetzes dabei die Sicherstellung verbindlicher Regelungen zur technischen Überwachung, Transparenz im Umgang mit datenverarbeitender künstlicher Intelligenz und der besondere Schutz der innerhalb eines Bewerbungsvorgangs erhobenen Daten. Dauerhafte Überwachung der Arbeitnehmer*innen soll lediglich im Ausnahmefall und unter engen Voraussetzungen zulässig sein. Darüber hinaus sieht das Positionspapier eine Konkretisierung der Anforderungen an die Freiwilligkeit einer Einwilligung zur Datenverarbeitung vor. Neben weitergehenden Regelungen zur gängigen BYOD („Bring Your Own Device“) Praxis, ist geplant, die Mitbestimmungsrechte und die kollektivrechtlichen Regelungen zu evaluieren und zu stärken. Zur Gewährleistung eines umfassenden Schutzes soll der sachliche Anwendungsbereich des Gesetzes dabei weit gefasst werden, so dass neben Arbeitnehmer*innen auch solo-selbständige Plattformtätige vom Schutzbereich des Gesetzes erfasst werden.

Eine klare gesetzliche Regelung und die Schaffung verbindlicher Rechtsgrundlagen ist sowohl aus Beschäftigtensicht als auch aus Arbeitgebersicht zu begrüßen. Es gilt jedoch zu beachten, dass im Datenschutzrecht die jeweiligen Interessen und geschützten Positionen sowohl der Arbeitnehmer*innen als die der Arbeitgeber*innen in Einklang zu bringen sind. Daher haben wir im Folgenden aufgeführt, was es bei den geplanten Regelungspunkten aus Sicht der Startups und Scaleups in Deutschland zu beachten gilt.

Anwendungsbereich klar definieren und Rechtssicherheit schaffen

Der Anwendungsbereich eines zukünftigen Beschäftigtendatenschutzgesetzes sollte klar abgesteckt und begründet sein. Die aktuellen Vorschläge sind noch recht weit gefasst, um möglichst viele Personen, die als Beschäftigte gelten könnten, in den Schutzbereich des Gesetzes einbeziehen zu können. Es sollte dabei jedoch unbedingt darauf geachtet werden, dass nur Personen, die in einem direkten Beschäftigtenverhältnis zu einem Unternehmen stehen, von dem Gesetz abgedeckt sind. Denn eine Ausweitung auf indirekte Beschäftigungsverhältnisse würde Arbeitgeber*innen vor große Herausforderungen stellen: so könnten datenschutzrechtliche Pflichten für Personen entstehen, für welche der Arbeitgeber keine tatsächliche Verantwortung trägt. Darüber hinaus würde eine zu weitreichende Definition dazu führen, dass Beschäftigte mehrere potenzielle Anspruchsgegner hätten. Dies könnte zu einer erhöhten Komplexität und Rechtsunsicherheit führen, da unterschiedliche Verantwortlichkeiten und Zuständigkeiten bestehen würden.

Ein konkretes Beispiel, in dem aktuell noch rechtliche Unsicherheiten bestehen, ist das Thema Salary Surveys. Diese Umfragen dienen der Ermittlung marktgerechter Gehälter und

sind gerade in Zeiten eines anspruchsvollen Bewerbermarktes ein wichtiger Bestandteil moderner Rekrutierungsprozesse. Aktuell erhalten Unternehmen in der Regel nur dann die erforderlichen Informationen, wenn sie ihre eigenen Mitarbeitergehälter offenlegen. Hier besteht jedoch eine erhebliche Unsicherheit darüber, ob eine solche Weitergabe von personenbezogenen Daten überhaupt datenschutzrechtlich zulässig ist. Das geplante Gesetz zum Beschäftigtendatenschutz sollte hier Klarheit schaffen, um Rechtssicherheit für Unternehmen und eine angemessene Balance zwischen Transparenz und Datenschutz zu gewährleisten.

Regelungen zur Freiwilligkeit der Einwilligung flexibel gestalten

Eine weitergehende Konkretisierung der Anforderungen an die Freiwilligkeit einer Einwilligung in die Datenverarbeitung im Beschäftigtenkontext ist aus Sicht von Startups und Scaleups allgemein positiv zu bewerten. Wichtig ist es dabei jedoch, sicherzustellen, dass durch die geplante Konkretisierung keine indirekte Pflicht zur Einwilligung oder eine Priorisierung dieser entsteht. Primäre Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten im Rahmen des Arbeitsverhältnisses ist grundsätzlich der Arbeitsvertrag. Daher sollte eine Konkretisierung vielmehr dazu führen, dass Arbeitgeber*innen klar und verständlich aufgezeigt wird, in welchen Situationen eine Einwilligung notwendig wird und unter welchen Voraussetzungen sie die Anforderungen der Freiwilligkeit erfüllt. Im Zuge der geplanten Konkretisierung sollten auch vom zwingenden Schrifterfordernis, an das Einwilligungen derzeitig noch geknüpft sind, abgesehen und auch digitale Wege ermöglicht werden. Diese würde die technologische Wirklichkeit vieler Unternehmen abbilden und dem alltäglichen Gebrauch der modernen, digitalen Kommunikationswege in den Unternehmen Rechnung tragen. Die Erweiterung der Einwilligungsmöglichkeit sollte dabei jedoch keine Beschneidung der Dokumentationspflichten zur Folge haben.

Balance zwischen Schutz der Beschäftigten vor Überwachung und Schutzpflichten der Arbeitgeber*innen gewährleisten

Der technologische Fortschritt, die sich daraus ergebende Weiterentwicklung und Veränderung der Arbeitsabläufe und die Ausweitung moderner Arbeitsformen stellt auch Arbeitgeber*innen vor neue Herausforderungen. Verbindliche Regelungen zur Überwachung und Kontrolle der Arbeitsabläufe sind aus unserer Sicht zunächst begrüßenswert, da sie Rechtssicherheit schaffen. Jedoch müssen diese Regelungen praxisnah sein und sollten das berechtigte Interesse der Arbeitgeber*innen an der Organisation und der Aufsicht über die Betriebsabläufe, sowie den Dokumentations- und Schutzpflichten der Arbeitgeber*innen nicht aus dem Blick verlieren. In dem Zusammenhang ist es wichtig, den genauen Anwendungsbereich der Regelungen auszudefinieren und - wo sinnvoll Arbeitgeber*innen einen größeren Ermessensspielraum zu gewähren. In folgenden Bereichen wäre in diesem Zusammenhang mehr Spielraum für Arbeitgeber*innen besonders wichtig:

- Konzerninterne Datenübermittlungen sollten im Rahmen eines Beschäftigtendatenschutzgesetzes weitgehend erlaubt sein, um die Skaleneffekte einer zentralisierten Datenverarbeitung bei der Konzernmutter nutzen zu können.

Übermäßige bürokratische Vorgaben, die keinen unmittelbaren Schutz für Beschäftigte bieten, belasten insbesondere junge Startups und Scaleups und beeinträchtigen die Agilität moderner wachstumsorientierter Unternehmen. Hier sollte eine ausgewogene Regelung gewählt werden, die die Privatsphäre der Beschäftigten schützt und zugleich interne Datenübermittlungen nicht ausschließt.

- Gängige Prozesse zur Qualitätskontrolle und -sicherung sowie zu Trainingszwecken in den Bereichen Sales und Vertrieb sollten durch die geplanten Vorgaben nicht eingeschränkt werden.
- Auch die Möglichkeit einer Durchführung von Umfragen zu Diversity, Equity und Inclusion ist für viele Unternehmen ein wichtiges Mittel, um Vielfalt und Integration zu fördern. Derzeit herrscht in diesem Bereich ein hohes Maß an Rechtsunsicherheit; auf der anderen Seite werden Maßnahmen zur Förderung von Vielfalt und Integration von vielen Bewerber*innen gewünscht. Es wäre daher aus unserer Sicht hilfreich, eine klare gesetzliche Regelung zur Erhebung der dafür notwendigen sensiblen personenbezogenen Daten nach Artikel 9 DSGVO zu schaffen – unter Bewahrung der entsprechenden Sicherheitsvorkehrungen und Schutzmechanismen.

Begriff der Datenverwertung präzisieren

Die im Positionspapier gewählte Formulierung (Punkt 9) „prozessuale Verwertungsverbote" wirft Fragen bzgl. der genauen Definition auf. Bis dato wird im Zusammenhang mit Daten beziehungsweise Datenschutz von „Verarbeitung" gesprochen. Die gewählte Formulierung „prozessuale Verwertungsverbote" erinnert in der Begrifflichkeit an die der Zivilprozessordnung und die im Urheberrecht übliche Verwertung von Daten. Hier muss der Anwendungs- und Regelungsbereich im weiteren Prozess klar definiert werden.

„Bring Your Own Device"-Lösungen zugunsten von Startups weiter ermöglichen und IT-Sicherheit erhöhen

Das geplante Gesetz soll zudem Konkretisierungen in Hinblick auf BYOD-Lösungen enthalten. Denn laut Positionspapier birgt die in der Praxis übliche Verwendung privater Laptops und Smartphones für dienstliche Zwecke die Gefahr des Zugriffs auf private Daten und wirft daher datenschutzrechtliche Fragen auf. Eine Klarstellung der BYOD-Regelungen ist aus unserer Sicht prinzipiell zu befürworten. Dabei muss jedoch die Komplexität des Themas im Blick behalten werden. Neuregelungen dürfen nicht zu praxisuntauglichen Vorgaben führen. Denn gerade Startups und Scaleups gelten unter Arbeitnehmer*innen als besonders flexibel, wenn es um maßgeschneiderte Home-Office-Regelungen und flexible Arbeitsweisen geht. Darüber hinaus arbeiten gerade junge Startups oft mit begrenzten Ressourcen und bieten aus diesem Grund zunächst BYOD-Lösungen an, um Kosten zu sparen. Diese besonderen Voraussetzungen von Startups müssen bei der Ausgestaltung von BYOD-Regelungen berücksichtigt werden.

Neben der Praxistauglichkeit stellt dabei die IT-Sicherheit die größte Herausforderung dar. Erlauben Arbeitgeber*innen aktuell den Beschäftigten den privaten Gebrauch dienstlicher Geräte, gelten die Arbeitgeber*innen als Telekommunikationsanbieter. Dieser Status verhindert IT-sicherheitsrelevante Maßnahmen und gefährdet damit letztlich auch die IT-Sicherheit der Beschäftigten und ihrer persönlichen Daten. Darüber hinaus können

Angreifer*innen gerade über Beschäftigte in das Unternehmen eindringen und mittels Ransomware ganze Unternehmensgruppen lahmlegen und erpressen. Solche Angriffe gefährden dann nicht nur Unternehmensdaten, sondern auch die Daten und Arbeitsplätze der Beschäftigten. Der Wettlauf der Technik erfordert einen wirksamen Schutz und die Möglichkeit, jede Verbindung ins und im Unternehmensnetzwerk auf solche Angriffe hin zu kontrollieren. Eine Einschränkung dieser Möglichkeit geht nicht nur zu Lasten der Arbeitgeber*innen, sondern auch zu Lasten der Arbeitnehmer*innen.

Doppelstrukturen durch Mitbestimmung von Betriebs- und Personalräten vermeiden

Das Positionspapier sieht vor, die Mitbestimmung von Betriebs- und Personalräten weiterzuentwickeln. Dafür soll insbesondere das Betriebsrätemodernisierungsgesetz mit Blick auf die Gestaltungrechte der Arbeitnehmer*innen bei der sozial-ökologischen Transformation und Digitalisierung evaluiert werden. Jedoch regelt bereits die EU-Datenschutzgrundverordnung, dass Datenschutz in der Verantwortung der Arbeitgeber*innen liegt. Dies wird durch die gesetzliche Aufforderung zur Bestellung eines Datenschutzbeauftragten durch die Arbeitgeberseite weiter bestärkt.
Sinn und Zweck des Betriebs- und Personalrats ist die Mitbestimmungsmöglichkeit und kann daher aus unserer Sicht in keinem Fall eine Überwachungsfunktion für den Datenschutz einnehmen. Denn anders als Arbeitgeber*innen und Datenschutzbeauftragte muss er sich weder für Fehler im Bereich des Datenschutzes verantworten, noch kann er aus solchen haftbar gemacht werden. Zudem ist festzuhalten, dass es Betriebs- und Personalräten oft auch an der fachlichen Kompetenz und Ressourcen fehlt, den "Stand der Technik" aufmerksam zu verfolgen. Dies ist auf Arbeitgeberseite durch den extra eingesetzten Datenschutzbeauftragten sichergestellt. Hinzu kommt, dass die Verarbeitung personenbezogener Daten im Zuge der betriebsrätlichen Arbeit bereits durch § 79a BtrVG geregelt wird, der die Bindung an die Vorschriften des Datenschutzes vorsieht. Somit würden durch eine weitreichende Mitbestimmung von Betriebs- und Personalräten beim Datenschutz Doppelstrukturen und rechtlichen Unklarheiten geschaffen werden
Eine Novellierung der Mitbestimmungsrechte der Arbeitnehmer*innen sollte daher die grundsätzliche Verantwortlichkeit gemäß den Anforderungen der DSGVO Rechnung tragen und keine widersprüchliche Zuständigkeit erschaffen.

Gestaltungsmöglichkeiten der kollektivrechtlichen Regelungen prüfen

Das Positionspapier sieht Betriebsvereinbarungen als Instrument zur Konkretisierung des Beschäftigtendatenschutzrechts vor und zielt darauf ab, die geltende Rechtslage für Kollektivvereinbarungen als Regelung für Datenverarbeitungen im Beschäftigungskontext zu prüfen. Dies wirft bereits zum jetzigen Zeitpunkt die Frage auf, ob Gestaltungsmöglichkeiten innerhalb von Betriebsvereinbarungen auch über die Regelungen der DSGVO hinaus möglich sind. Hier sollten die zuständigen Ministerien im weiteren Prozess weiter erörtern, in welchen Bereichen Betriebsvereinbarungen erforderlich und möglich sind und wo sie nicht notwendig sind. Dies sollte möglichst konkret ausgestaltet sein, um Rechtsunsicherheiten zu vermeiden.

Zertifizierung gängiger Tools und Prüfung der Datenschutz-Folgeabschätzung

Um den mit dem technologischen Fortschritt steigenden Anforderungen an die Arbeitgeber*innen gerecht werden zu können, ist es nötig, die Umsetzung des Datenschutzes möglichst praxisnah und, wo möglich, unkompliziert zu gestalten. Das geplante Beschäftigtendatenschutzgesetz bietet die Möglichkeit, eine generelle datenschutzrechtliche Zertifizierungen verschiedener Tools, beispielsweise HR-Software oder KI-Anwendungen rechtlich einzubinden. Diese würden die datenschutzrechtliche Prüfung im Beschaffungsprozess erheblich erleichtern. Unternehmen könnten so schon bei der Beschaffung sicherstellen, dass die genutzten Tools den datenschutzrechtlichen Vorgaben entsprechen.

Interne, sich gleichende Verarbeitungsprozesse sollten darüber hinaus zur Erleichterung der betrieblichen Organisation von der Datenschutz-Folgeabschätzung gemäß Artikel 35 DSGVO befreit werden, wenn eine solche für vergleichbare Abläufe vorliegt. Die Ausarbeitung der Folgenabschätzung für die einzelnen Vorgänge erfordert schon jetzt erhebliche Ressourcen und bindet deutliche Kapazitäten. Für eine sich an den Anforderungen der technischen Entwicklung anpassenden, agile und effiziente Arbeitsweise ist der Abbau vergleichbarer Vorgänge, die auch durch eine Gesamtabschätzung erfasst werden könnten, elementar.

Ebenfalls sollten Anwendungen den Datenschutz durch Technikgestaltung und durch Voreinstellungen sicherstellen. Grundsätzlich wäre es wünschenswert wenn der Gesetzgeber einen Kriterienkatalog bereitstellen würde, anhand welchem die Arbeitgeber*innen geeignete Tools auswählen können. Die Kriterien sollten dabei konkret auf den Beschäftigtendatenschutz abzielen und die grundsätzlichen Anforderungen der DSGVO ergänzen.

Vorhaben im weiteren Prozess konkretisieren und angemessene Fristen zur Kommentierung gewähren

Das geplante Gesetz bietet begrüßenswerte Ansätze, die sowohl für Arbeitgeber*innen als auch Arbeitnehmer*innen weitere Rechtssicherheit schaffen können. Auf der anderen Seite bergen einige der Vorhaben die Gefahr, die Arbeitgeberseite stark zu belasten und somit insbesondere für kleine Unternehmen mit weniger Ressourcen Nachteile zu schaffen. Wir halten daher eine praxisnahe Ausgestaltung der Regelungen für äußerst wichtig. Im ersten Schritt sollten die Vorschläge dazu im weiteren Prozess konkretisiert werden, damit eine abschließende Beurteilung möglich ist. Besonders ist es uns dabei wichtig, eine angemessen lange Frist zur Kommentierung eines Referentenentwurfs zu erhalten, um die Vorschläge aus Startup- und Scaleup-Sicht tiefgehend prüfen zu können.

Der Startup-Verband

Der Bundesverband Deutsche Startups e.V. ist die Stimme der Startups in Deutschland. Seit seiner Gründung 2012 vertritt der Verband die Startup-Interessen gegenüber Politik, Wirtschaft und Öffentlichkeit.
In seinem Netzwerk mit mittlerweile 1.200 Mitgliedern schafft der Verband darüber hinaus einen Austausch zwischen Startups untereinander, ab er auch zwischen Startups und etablierter Wirtschaft. Ziel des Startup-Verbandes ist es, Deutschland und Europa zu einem gründungsfreundlichen Standort zu machen, der Risikobereitschaft honoriert und den Pionier*innen unserer Zeit die besten Voraussetzungen bietet, um mit Innovationskraft erfolgreich zu sein.