bidt Bayerisches Forschungsinstitut für Digitale Transformation
EIN INSTITUT DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN

IMPULSE

Mehr ist mehr:

Besserer Beschäftigtendatenschutz für umfassende Nutzung von Arbeitsplatzdaten

Autor:in
Mena Teebken
Thomas Hess

Impressum

bidt Impulse Nr. 6

bidt – Bayerisches Forschungsinstitut
für Digitale Transformation
Gabelsbergerstraße 4
80333 München
www.bidt.digital

Redaktionelle Koordination
Leonie Liebich, Dr. Margret Hornsteiner
dialog@bidt.digital

Gestaltung
made in – Design und Strategieberatung
www.madein.io

Veröffentlichung
Januar 2024

ISSN: 2701-2395
DOI: 10.35067/b0bj-im06

Das Bayerische Forschungsinstitut für Digitale Transformation (bidt) trägt als Institut der Bayerischen Akademie der Wissenschaften dazu bei, die Entwicklungen und Herausforderungen der digitalen Transformation besser zu verstehen. Damit liefert es die Grundlagen, um die digitale Zukunft der Gesellschaft verantwortungsvoll und gemeinwohlorientiert zu gestalten.

In der heutigen Arbeitswelt, die zunehmend von digitalen Technologien durchdrungen ist, gewinnt der Schutz von Beschäftigtendaten an Bedeutung. Trotz existierender Regelungen zum Umgang mit Beschäftigtendaten bleibt der aktuelle Beschäftigtendatenschutz fragmentiert und muss an die dynamischen Anforderungen einer digitalisierten Arbeitswelt angepasst werden. In diesem „bidt Impuls" beleuchten Dr. Mena Teebken und Professor Thomas Hess die zentralen Herausforderungen des Datenschutzes am Arbeitsplatz und bieten konkrete Empfehlungen, um sowohl das Vertrauen der Beschäftigten in den Datenschutz zu stärken, als auch die Bedürfnisse der Unternehmen effektiv zu adressieren. Sie argumentieren, dass ein umfassender und ausgeglichener Ansatz im Beschäftigtendatenschutz nicht nur die Privatsphäre der Beschäftigten schützt, sondern auch ein Schlüsselelement für den Erfolg in unserer zunehmend datengetriebenen Arbeitswelt darstellt.

Autor:in

Dr. Mena Teebken ist wissenschaftliche Referentin am bidt.
E-Mail: mena.teebken@bidt.digital

Prof. Dr. Thomas Hess ist Mitglied im bidt Direktorium und Professor für Wirtschaftsinformatik und Betriebswirtschaftslehre an der Ludwig-Maximilians-Universität München.
E-Mail: thomas.hess@bidt.digital

Abstract

Im digitalen Zeitalter ist der Datenschutz am Arbeitsplatz entscheidend für die Balance zwischen Beschäftigtenprivatsphäre und Unternehmensinteressen. Während Beschäftigtendaten für betriebliche Effizienz unerlässlich sind, fordert der fragmentierte Beschäftigtendatenschutz eine Überarbeitung. Dieser „bidt Impuls" betont die Notwendigkeit einer ganzheitlichen Sicht auf Datenschutz, die sowohl Beschäftigten- als auch Unternehmensbedürfnisse einbezieht.

Aus ihrer Studie über Beschäftigtenperspektiven zur Privatsphäre leiten die Autorin und der Autor fünf Datenschutzherausforderungen ab, die alle Phasen des Datenlebenszyklus am Arbeitsplatz abdecken: Generierung von Daten, deren Analyse und Verarbeitung, Speicherung, interne und externe Empfänger sowie die Umsetzung der Regulation im Unternehmen. Daraus folgen fünf Empfehlungen: verantwortungsbewusste Datenerfassung, Sicherstellung von Haftung und Transparenz bei KI-Nutzung, klare Begrenzung der Datenspeicherung, Gewährleistung des Datenschutzes für interne und externe Empfänger sowie die Förderung von Transparenz und Sensibilisierung der Beschäftigten. Diese Maßnahmen sollen das Vertrauen in den Datenschutz stärken, was wiederum die Bereitschaft der Beschäftigten erhöht, Daten freizugeben.

Der „bidt Impuls" unterstreicht, dass effektiver Beschäftigtendatenschutz sowohl die Privatsphäre schützt, als auch Vorteile für Unternehmen bietet. Zudem hebt er die Bedeutung von Datenschutz als Vertrauens- und Erfolgsfaktor in der digitalen Arbeitswelt hervor.

Inhalt

01

Einleitung

In einer zunehmend digitalisierten Arbeitswelt, die von der umfassenden Generierung und Verarbeitung von Beschäftigtendaten geprägt ist, hat das Thema Datenschutz und die damit verbundene Privatheit der Beschäftigten eine immense Bedeutung. Beschäftigtendaten sind aus verschiedenen Gründen von erheblichem Interesse für Unternehmen. Sie bieten Einblicke in Arbeitsgewohnheiten und -leistungen und bilden damit die Grundlage für die Steigerung der betrieblichen Effizienz und Produktivität und letztlich zur Sicherung der Wettbewerbsfähigkeit.

Darüber hinaus liefern Daten wertvolle Informationen, die als Grundlage für fundierte Entscheidungen dienen und somit die Zukunft unserer Arbeitswelt maßgeblich beeinflussen, beispielsweise durch die Automatisierung von Arbeitsprozessen. Gleichzeitig müssen die berechtigten Interessen der Beschäftigten bezüglich der am Arbeitsplatz gesammelten Daten gewahrt bleiben. Die richtige Balance zwischen den Interessen von Unternehmen und Beschäftigten ist daher entscheidend. Erforderlich ist somit ein Weg im Umgang mit Beschäftigtendaten, der den Interessen der Unternehmen und der Beschäftigten gerecht wird.

Die Autorin und der Autor sind der Ansicht, dass die tatsächliche Wahrnehmung der Beschäftigten bei bisherigen Evaluierungen des Beschäftigtendatenschutzgesetzes nur unzureichend berücksichtigt wurde. Meinungen, Bedenken und Bedürfnisse der Beschäftigten, die im Zentrum der Datenschutzdebatten stehen, werden nicht ausreichend einbezogen. Daher ist es notwendig, einen umfassenden Ansatz zur Evaluation des Beschäftigtendatenschutzes zu finden, der die verschiedenen Aspekte miteinander verknüpft und die Perspektive der Beschäftigten angemessen berücksichtigt.

In diesem „bidt Impuls“ verfolgen die Autorin und der Autor einen ganzheitlichen Ansatz, der die tatsächliche Wahrnehmung der Beschäftigten in den Mittelpunkt rückt, um einen effektiveren und ausgewogeneren Schutz der Rechte und Interessen aller Beteiligten zu gewährleisten.

Hinweis

Die Inhalte des vorliegenden „bidt Impuls“ sind eine verkürzte Darstellung der im Sommer 2023 publizierten Studie von Teebken, Constantiou und Hess (2023). Diese Zusammenfassung stützt sich primär auf die Daten und Erkenntnisse des genannten Papers, während tiefergehende Interpretationen und Analysen auf der Dissertation von Teebken (2023) basieren, die eine umfassendere Betrachtung der Thematik bietet. Für detailliertere Ausführungen und Begründungen wird auf die vollständige Dissertation verwiesen. Zudem ist Teebken Mitarbeiterin des bidt-Forschungsprojekts „Determinanten der Datenpreisgabe am digitalen Arbeitsplatz“, das untersucht, inwiefern unterschiedliche Faktoren der digitalen Arbeit die Bereitschaft zur Datenpreisgabe beeinflussen.

02

Die Diskussion um die Weiterentwicklung des Beschäftigten-datenschutzes

Der regulative Rahmen ist von zentraler Bedeutung für den individuellen Weg, den jedes Unternehmen in Bezug auf den Beschäftigtendatenschutz beschreiten muss. Ein wesentliches Element des Datenschutzregimes in Deutschland und der Europäischen Union ist die Datenschutz-Grundverordnung (DSGVO), die seit ihrer Einführung im Jahr 2018 maßgebliche Vorgaben für den Umgang mit personenbezogenen Daten setzt. Neben dem Bundesdatenschutzgesetz (BDSG), das in seiner Neufassung von 2018 spezifische Regelungen zum Datenschutz am Arbeitsplatz enthält, und dem Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) spielt auch das Betriebsverfassungsgesetz (BetrVG) im Arbeitsplatzkontext eine wichtige Rolle.

DSGVO
Datenschutz-Grundverordnung

BDSG
Bundesdatenschutzgesetz

TTDSG
Telekommunikations-Telemedien-Datenschutz-Gesetz

BetrVG
Betriebsverfassungsgesetz

2.1 Fragmentierung und Modernisierungsbedarf

Insgesamt ist festzuhalten, dass in Deutschland derzeit kein spezifisches Gesetz existiert, das ausschließlich den Datenschutz von Beschäftigten regelt (Beschäftigtendatenschutz 2020; BfDI 2023; Datenschutzexperte 2023). Stattdessen sind relevante Bestimmungen über verschiedene Gesetze verteilt. Als Resultat ist der aktuelle Beschäftigtendatenschutz fragmentiert und nicht mehr zeitgemäß (Schwemmle/Wedde 2018; Tolsdorf 2022). Somit besteht ein deutlicher Bedarf an spezifischeren, klareren und praxisorientierten Regelungen, um den Herausforderungen des Datenschutzes am Arbeitsplatz effektiv zu begegnen. Obwohl die Einführung eines konkreten Beschäftigtendatenschutzgesetzes seit einiger Zeit an-

gekündigt wird, haben trotz zahlreicher Bemühungen nur begrenzte Fortschritte stattgefunden (Rusch 2023; Nanos 2023).

2.2 Initiativen und Zukunftspläne

Bereits in der Datenstrategie 2021 wird dem Beschäftigtendatenschutz eine grundlegende Rolle und aktuelle Relevanz zugesprochen. Im Januar 2021 initiierte der Beirat zum Beschäftigtendatenschutz des Bundesministeriums für Arbeit und Soziales eine eingehende Prüfung der Anforderungen an die Weiterentwicklung des Beschäftigtendatenschutzes. Als Reaktion auf die Ergebnisse dieser Prüfung veröffentlichten das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Inneren und für Heimat (BMI) im April 2023 ein Eckpunktepapier zur Überarbeitung des Beschäftigtendatenschutzes. Dieses Eckpunktepapier zielt darauf ab, Lösungen für Herausforderungen im Umgang mit Beschäftigtendaten zu erarbeiten und rechtliche Unsicherheiten abzubauen. Dazu gehört die Erweiterung des Beschäftigtenbegriffs, die Regulierung von Überwachung und Kontrolle der Beschäftigten sowie die Schaffung von Transparenz beim Einsatz von künstlicher Intelligenz. Die Bedeutung des Beschäftigtendatenschutzes spiegelt sich erneut in der Roadmap der Datenstrategie der Bundesregierung 2023 wider, die das vierte Quartal 2023 als das angestrebte Ziel für die Einführung des überarbeiteten Beschäftigtendatenschutzgesetzes festlegt. Diese zeitliche Zielsetzung unterstreicht die wachsende Relevanz des Themas.

Die oben erwähnten ersten Schritte zur Überarbeitung des Beschäftigtendatenschutzes konzentrieren sich in erster Linie auf einzelne Aspekte, die auf verschiedenen Ebenen der Gesetzgebung und Regulierung adressiert werden. Dies führt dazu, dass die Wechselwirkungen dieser Aspekte oft vernachlässigt werden, was eine ganzheitliche Bewertung erschwert.

03

AUFBAU VON VERTRAUEN:

Eine Alternative zur Absenkung der Regulation

In der Diskussion um den Umgang mit Datenschutz in Unternehmen treten immer wieder zwei tendenziell widersprüchliche Positionen hinsichtlich der Ausgestaltung der Balance zwischen Datennutzung und Regulierung hervor (Martin et al. 2019).

Ansatz der Datensparsamkeit

1

Traditionell dominiert in Deutschland der Ansatz der Datensparsamkeit, der die Minimierung von Daten zur Wahrung der Privatheit propagiert. Dieser Ansatz fordert, dass Unternehmen verpflichtet sein sollten, strenge Regulation einzuhalten, um die Privatsphäre und die Grundrechte von Individuen zu wahren (Meckel 2023).

Position der gelockerten Regulierung

2

Demgegenüber werden Stimmen lauter, die fordern, die Regulierung von Unternehmen zurückzufahren, um so die Wettbewerbsfähigkeit der Unternehmen im internationalen Wettbewerb zu fördern (Wallace/Castro 2018). Befürworter dieser Position argumentieren, dass weniger Regulation mehr Spielraum für Unternehmen schafft. Weniger Vorschriften bedeuten hier, dass Unternehmen schneller auf Veränderungen reagieren und neue Technologien einsetzen können, ohne durch rigide Datenschutzanforderungen in ihren Handlungsspielräumen eingeschränkt zu werden oder sich mit komplexen Gesetzeslagen auseinandersetzen zu müssen.

Vertrauen durch Schutz: Wie Regulierung die Datenfreigabe fördert

3

Zum Einfluss der Regulation auf Datenpreisgabe gibt es mittlerweile empirische Forschung, die zeigt: Wenn Individuen das Vertrauen haben, dass ihre Daten angemessen geschützt sind, werden ihre Bedenken bezüglich ihrer Privatsphäre signifikant verringert (Xu et al. 2012). Weniger Privatheitsbedenken wirken sich beispielsweise positiv auf das Vertrauen (Acquisti et al. 2015) oder die Bereitschaft aus, Daten zur Verfügung zu stellen (Cichy et al. 2021). Somit schafft eine verbesserte Regulierung klare und verlässliche Rahmenbedingungen, die für Arbeitgeber und Beschäftigte gleichermaßen von Vorteil sein können. Die Forschung legt nahe, dass eine angemessene und zielgerichtete Regulierung nicht nur die Privatheit gewährleisten, sondern im Sinne der Datenstrategie auch die Grundlage für verstärkte Datenpreisgabe legen kann.

04

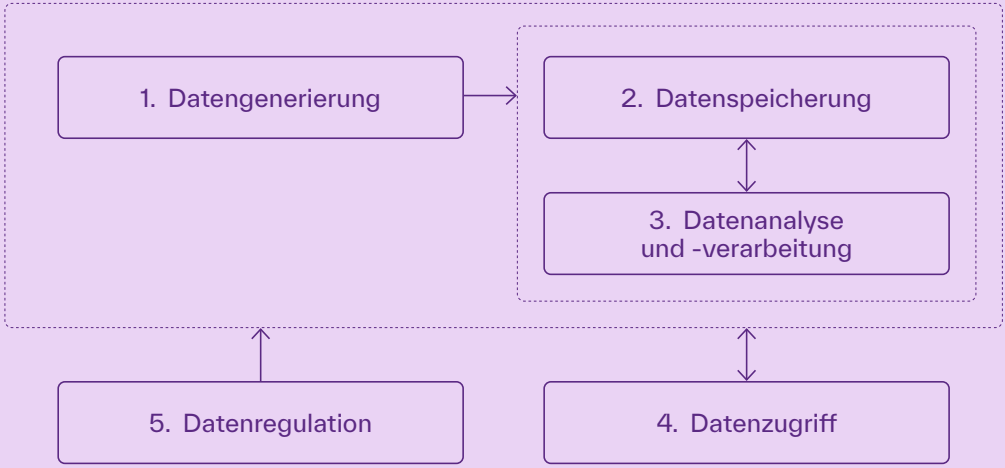
BESCHÄFTIGTENPERSPEKTIVEN:

Die top fünf Datenschutz-herausforderungen

Die Studie von Teebken, Constantiou und Hess (2023) hat im Rahmen von Interviews mit Beschäftigten deren Wahrnehmung von Privatheit am digitalen Arbeitsplatz untersucht.* Die Ergebnisse dieser Befragungen offenbarten trotz bestehender Datenschutzregulierungen erhebliche Privatheitsbedenken bei Beschäftigten, wenn sie digital arbeiten. Es konnten fünf konkrete Bereiche im Umgang mit Beschäftigtendaten identifiziert werden, die von Beschäftigten als besonders problematisch wahrgenommen werden. Diese Schlüsselpunkte sind in der Abbildung auf Seite 20 zusammengefasst und folgen der Logik der Datenlebenszyklen am Arbeitsplatz. Im folgenden Abschnitt werden diese Bereiche im Detail beleuchtet.

* In der Studie wurden die Perspektiven von 66 Beschäftigten aus verschiedenen Industrien und Disziplinen zur Wahrnehmung von Privatheit und Datenschutzbedenken am digitalen Arbeitsplatz eingehend untersucht. Die Teilnehmenden der Umfrage stammen aus einer breiten Palette an Bildungshintergründen, Berufsdisziplinen, Industriezweigen und demografischen Merkmalen, was der Studie eine hohe Repräsentativität verleiht. Die Ergebnisse bieten einen tiefgreifenden Einblick in die vielschichtigen Auffassungen und Bedenken der Beschäftigten in Bezug auf ihre Privatsphäre am Arbeitsplatz in der digitalisierten Welt. Im folgenden Text werden direkte Zitate aus den Interviews in Anführungszeichen wiedergegeben. Weitere detaillierte Informationen zu dieser Studie sowie zu ähnlichen Forschungsarbeiten finden sich in der Dissertation von Teebken (2023).

Beschäftigtendatenlebenszyklus am digitalen Arbeitsplatz



Generierung von Beschäftigtendaten

1

Mitarbeitende haben erhebliche Bedenken hinsichtlich der **Art der generierten Beschäftigtendaten**. Diese Bedenken manifestieren sich in der mangelnden expliziten **Einwilligung** bei der Datenerhebung, der **übermäßigen Sammlung** von Daten über das notwendige Maß hinaus und der Erfassung äußerst sensibler Informationen im beruflichen Umfeld. Dazu gehören beispielsweise Finanzdaten, Gesundheitsdaten, Produktivi-

tätsdaten oder Leistungsbeurteilungen. Dies führt dazu, dass „die Grenzen zwischen Privat- und Berufsleben verschwimmen“. Die Studienteilnehmenden betonten, dass die **Art der Daten**, die bei der digitalen Arbeit offengelegt werden, ihre Wahrnehmung der Privatsphäre beeinflusst: „Das beunruhigt mich, weil einige dieser Informationen vertraulich sind und es sich um meine persönlichen Informationen handelt.“ Ebenso haben Beschäftigte Bedenken wegen eines **Kontrollverlusts** über die automatisierte Datensammlung, was zu einer potenziellen Verletzung der Privatsphäre führt.

2 Analyse und Verarbeitung von Beschäftigtendaten

Auch bezüglich der **Analyse und Verarbeitung ihrer Daten** zeigt die Studie Privatheitsbedenken der Beschäftigten auf. Besonders kritisch wird die Verwendung digitaler Daten am Arbeitsplatz im Zusammenhang mit **Überwachung und Leistungsbeurteilung** der Handlungen der Beschäftigten gesehen. Die Befragten äußerten verschiedene negative Gefühle im Zusammenhang mit der Nutzung persönlicher Daten durch den Arbeitgeber. Ein Teilnehmender artikuliert: „Je mehr Daten über mich gesammelt werden, desto mehr Daten hat der Arbeitgeber, um potenziell damit gewisse Maßnahmen zu ergreifen, also beispielsweise – rein theoretisch – zu überwachen oder Rückschlüsse auf alles Mögliche, was die Arbeit angeht, was das Arbeitsverhalten angeht, zu ziehen.“ Dieser Kontext stellt daher eine der dringlichsten Herausforderungen für den Schutz der Privatsphäre dar. Zudem werden die Anwendung von

künstlicher Intelligenz und die Verknüpfung von Datenpunkten, die zu umfassenden Mitarbeiterprofilen führen, mit Bedenken betrachtet: „Es wird alles völlig transparent. Und damit meine ich, dass mein Arbeitgeber im Grunde alles sehen kann, was ich mit Technologien während digitaler Arbeit mache."

3 Speicherung von Beschäftigtendaten

Beschäftigte äußern erhebliche Bedenken in Bezug auf die Speicherung ihrer Daten. Dazu gehören Bedenken hinsichtlich der Datenspeicherdauer, der Struktur der Datenspeicherung (Cloud versus On-Premise) und des geografischen Ortes, an dem die Daten gespeichert werden. Insbesondere die Speicherung von Daten außerhalb der Europäischen Union stellt eine zusätzliche Herausforderung dar und erzeugt Datenschutzbedenken. Dabei steht die Wahrnehmung der Privatsphäre in direktem Zusammenhang mit dem Ort der Speicherung und der entsprechenden Regulierung in den jeweiligen Ländern. „Aber prinzipiell habe ich Probleme damit, wenn Clouddienste in den USA das machen (Daten speichern), weil das Regelwerk da drüben noch laxer ist als hier." Dies betrifft nicht nur die Speicherung von Daten durch den Arbeitgeber, sondern insbesondere die Datenspeicherung durch (Dritt-)Anbieter digitaler Lösungen. „Ich habe zum Beispiel auch ein, zwei Softwares aus China und da bin ich doch sehr, sehr vorsichtig."

Interne und externe Empfänger von Beschäftigtendaten

4

Beschäftigte haben erhebliche Sorgen bezüglich der **internen und externen Empfänger ihrer Daten**. Hierzu gehört die Befürchtung, dass **unautorisierte Akteure** Zugang zu ihren privaten Daten erhalten könnten. Intern spielen Arbeitgeber, Kolleginnen und Kollegen und die IT-Abteilung eine wichtige Rolle beim Datenzugriff und der anschließenden Datennutzung, was Datenschutzbedenken aufwirft. Neben den Dienstleistern machen die Mitarbeitenden auch unbekannte Parteien, die eigentlich keinen Zugang zu personenbezogenen Daten haben sollten, für Datenschutzprobleme verantwortlich. Externe Empfänger wie Serviceprovider, Geschäftspartner und potenzielle Hacker erzeugen zusätzliche Bedenken hinsichtlich des Datenschutzes. Dazu gehören beispielsweise auch Geschäftskunden. „Somit ist da schon mein Bedenken, dass der Kunde gegebenenfalls Zugriff auf Daten hat, die ihn eigentlich erstmal primär nichts angehen." Beschäftigte sind besorgt darüber, dass die Sichtweise auf Datenschutzrechte je nach den involvierten Interessenvertreterinnen und -vertretern variieren kann, was zu Inkonsistenzen führt.

Umsetzung der Regulation im Unternehmen

5

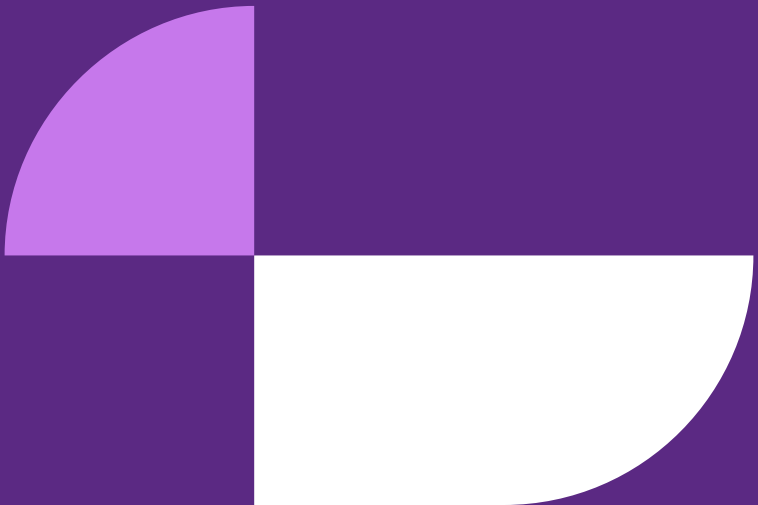
Auch hinsichtlich der **Umsetzung von Datenschutzregulationen** im Unternehmen haben Beschäftigte besondere Bedenken. Dies äußert sich in Unsicherheit bezüglich der Rolle von **Gewerkschaften**, dem Vorhandensein von Datenschutzrichtlinien für Mitarbeitende und bei der **Gewährleistung der Privatsphäre** im Unternehmen. Wie Datenschutz am Arbeitsplatz durch die Beschäftigten wahrgenommen wird, hängt maßgeblich davon ab, welchen Eindruck sie von der **Wirksamkeit staatlicher Regelungen** haben. In Deutschland stützt sich das Regelwerk der Rechte am Arbeitsplatz auf die allgemeinen Rechte der Betroffenen und die nationalen Arbeitsschutzgesetze. Beschäftigte fühlen sich vor dem Missbrauch personenbezogener Daten geschützt, wenn sie die Regelungen als wirksam wahrnehmen. „Du musst dich dann halt darauf verlassen, was das Unternehmen angibt oder einfach, dass sie die DSGVO befolgen." Auf internationaler Ebene betonen die Beschäftigten ihr Vertrauen in die Strafverfolgung von Unternehmen bei unrechtmäßigem Verhalten. „Was jetzt dazu beiträgt, dass ich relativ wenig Bedenken habe, ist, dass man manchmal von Unternehmen oder großen Konzernen und deren Klagen hört, weil jemand überwacht wurde oder jemandem eine Mitteilung über etwas zugestellt wurde."

Die beschriebenen Privatheitsbedenken der Beschäftigten am digitalen Arbeitsplatz unterstreichen die Notwendigkeit einer umfassenden und maßgeschneiderten Regulation im Bereich des Beschäftigtendatenschutzes. Der Einbezug der Beschäftigtenperspektive in den Gesetzgebungsprozess ist von entscheidender Bedeutung, um zu einem ausgewogenen und effektiven Schutz der Privatsphäre am Arbeitsplatz zu gelangen.

05

AUFBAU VON VERTRAUEN ALS NEUE ZIELRICHTUNG:

Fünf Empfehlungen für die Anpassung des Beschäftigungs-datenschutzes



Zuvor wurden fünf Aspekte beschrieben, die Beschäftigte kritisch beurteilen. Dies bedeutet aber auch: Vermeidet man diese, dann gewinnen Beschäftigte Vertrauen. Nachfolgend finden sich auf Basis der Interviews fünf Vorschläge, mit deren Hilfe sich das Gesetz zum Beschäftigungsdatenschutz zum Treiber für den Aufbau von Vertrauen umbauen lässt.

Datenerfassung verantwortungsbewusst steuern

1

Beschäftigte fordern klare Regelungen, die übermäßige Datensammlung einschränken und sicherstellen, dass nur **relevante und notwendige** Daten erfasst werden. In der Praxis bleibt oft **unklar**, welche Daten als relevant und notwendig gelten, was zu einer übermäßigen Datenerhebung führt. Zudem bestehen Bedenken hinsichtlich der **expliziten Einwilligung** bei der Generierung von Daten. Der Gesetzgeber sollte **klare Richtlinien** oder Beispiele bereitstellen, welche Daten als relevant und notwendig für die Arbeitserfüllung angesehen werden. Dies könnte durch **Leitfäden oder spezifische Anwendungsfälle** erfolgen, die es Unternehmen erleichtern, die Prinzipien der Datenminimierung und Zweckbindung korrekt anzuwenden.

Haftung und Transparenz sicherstellen

2

Transparenz und Erklärbarkeit sind für Beschäftigte beim Einsatz von KI-Technologien und Datenverarbeitung von großer Bedeutung. Die **Komplexität der KI-Technologien** und die Schwierigkeit der Zuweisung von **Verantwortung** führen zu Herausforderungen, insbesondere bei selbstlernenden KI-Systemen, die Entscheidungen ohne direkte menschliche Einflussnahme treffen. Als Antwort auf die Bedenken von Beschäftigten sollte ein klarer gesetzlicher Rahmen geschaffen werden, der regelt, wer bei **Fehlern oder Missbrauch von KI-Systemen** haftbar ist. Ebenso sollten ethische **Standards für**

den Einsatz von KI am Arbeitsplatz entwickelt werden, die sicherstellen, dass KI-Systeme fair, unvoreingenommen und im Interesse der Beschäftigten eingesetzt werden. Die Umsetzung dieser Forderungen und Standards erfordert eine sorgfältige Balance zwischen dem Schutz der Rechte der Beschäftigten und der Förderung technologischer Innovationen. Eine **kontinuierliche Anpassung** und Überprüfung der gesetzlichen Rahmenbedingungen sind daher notwendig, um mit den sich schnell entwickelnden KI-Technologien Schritt zu halten und gleichzeitig die Rechte und Interessen der Beschäftigten zu wahren.

Datenspeicherung klar begrenzen

3

Beschäftigte sind über Art, Umfang und Ort der Datenspeicherung besorgt – gerade im internationalen Kontext. **Unklare und inkonsistente rechtliche Rahmenbedingungen** für die Datenspeicherung erschweren die Umsetzung von Vorgaben, besonders für kleinere Unternehmen mit begrenzten Ressourcen. Die Regulierung sollte klare Vorgaben zur **Dauer der Datenspeicherung** setzen. Insbesondere klare Richtlinien und Abkommen zur **internationalen Übertragung von Beschäftigtendaten** in einer global vernetzten Arbeitsumgebung sind notwendig. Diese sollten sicherstellen, dass Daten, die über Landesgrenzen hinweg übertragen werden, adäquaten Schutz genießen.

Datenschutz für interne und externe Empfänger gewährleisten

4

Beschäftigte sind besorgt über den Schutz ihrer Daten vor unbefugtem Zugriff durch interne und externe Empfänger. Unternehmen müssen sicherstellen, dass nur **berechtigte Personen Zugriff** auf sensible Daten haben, was in der Praxis schwer umsetzbar sein kann. Es ist komplex, die **Zugriffskontrolle** auf Daten durch interne und externe Empfänger zu gewährleisten, insbesondere wenn externe Parteien beteiligt sind. Zudem ist die Überwachung der Einhaltung von Datenschutzbestimmungen durch externe Dienstleister und Geschäftspartner herausfordernd. Auf der einen Seite sollten Arbeitgeber klare Regeln und Vertragsbedingungen für externe Dienstleister und Geschäftspartner festlegen, um die Einhaltung der Datenschutzbestimmungen zu gewährleisten. Auf der anderen Seite sollte der Gesetzgeber detaillierte Richtlinien oder Standards für die Zugriffskontrolle auf Daten festlegen.

Beschäftigte sensibilisieren, Transparenz fördern

5

Für Beschäftigte ist die Einschätzung der Privatsphäre komplex und sie kritisieren oft **mangelnde Transparenz** im Umgang mit ihren Daten. Eine detailliertere und verständlichere Orientierung zur Bewertung der Privatsphäre und zur Schaffung von mehr Transparenz bei der Verarbeitung von Beschäftigtendaten ist notwendig. Der Gesetzgeber kann die **Datenschutzgesetze vereinfachen und verständlichere Anleitungen**

bereitstellen. Dies könnte die Verwendung einfacher Sprache und praktischer Beispiele beinhalten, um das Verständnis zu erleichtern. Zudem sind eindeutige Anleitungen zur Rolle von Gewerkschaften, Datenschutzschulungen und internem Datenschutz erforderlich, um die aktive Beteiligung und das Bewusstsein der Beschäftigten im Datenschutzprozess zu stärken. Dies umfasst die Einrichtung von **konkreten Verfahren und Etablierung von Ansprechpartnerinnen und -partnern** für Datenschutzbelange, wodurch eine kontinuierliche und effektive Umsetzung des Datenschutzes am Arbeitsplatz gewährleistet wird.

Eine ganzheitliche Betrachtung dieser Felder ist wichtig, da sie ineinandergreifen und die Privatsphäre von Beschäftigten auf verschiedenen Ebenen beeinflussen. Eine Regulation, die nur eines dieser Problemfelder adressiert, führt zu einem unzureichenden Schutz der Privatsphäre, da die anderen Aspekte ungelöst bleiben. Eine umfassende Datenschutzregulierung sollte daher sicherstellen, dass alle Phasen des Datenlebenszyklus und insbesondere auch die Wahrnehmung der Beschäftigten berücksichtigt werden, um die Privatsphäre und die Rechte der Beschäftigten angemessen zu schützen.

06

FAZIT:

Weniger Bedenken, mehr Daten, größerer Spielraum für Unternehmen

Die dargestellten Privatheitsbedenken der Beschäftigten bieten Einblicke in die Bedürfnisse und Erwartungen zum Beschäftigtendatenschutz. Dabei ist es von entscheidender Bedeutung bei der zukünftigen Ausgestaltung des Beschäftigtendatenschutzgesetzes, die Perspektive der Beschäftigten in den Mittelpunkt der Diskussion zu stellen, da sie nicht nur die Schutzadressaten sind, sondern auch diejenigen, die unmittelbar von den Auswirkungen betroffen sind. Trotz bestehender Datenschutzmaßnahmen offenbarten Interviews mit Beschäftigten signifikante Privatsphärebedenken beim digitalen Arbeiten. Fünf Hauptanliegen wurden identifiziert: Datenerzeugung, -analyse, -speicherung, Datenempfänger und die Umsetzung von Regulierungen.

Auf Grundlage dieser Erkenntnisse lassen sich gezielte Empfehlungen ableiten, die für Arbeitnehmerinnen und Arbeitnehmer besonders relevant sind: verantwortungsvolle Datenerfassung, Transparenz und Haftung bei KI-Einsatz, klare Grenzen für Datenspeicherung, Datenschutz bei internen und externen Empfängern sowie Förderung von Transparenz und Sensibilisierung. Diese Maßnahmen sollen nicht nur das Vertrauen in den Datenschutz stärken, sondern auch die Bereitschaft zur Datenfreigabe bei den Beschäftigten erhöhen.

Dieser „bidt Impuls“ hebt die zentrale Rolle eines Datenschutzes am Arbeitsplatz hervor, der dazu beiträgt, die Privatheitsbedenken der Beschäftigten zu reduzieren. Diese Reduktion von Bedenken wiederum schafft ein gesteigertes Vertrauen der Beschäftigten sowohl in den Schutz ihrer persönlichen Daten als auch in die datengetriebenen Prozesse am Arbeitsplatz. Die Erkenntnisse aus der Forschung zeigen, dass ein höheres Maß an Datenschutz die Bereitschaft der Beschäftigten erhöht, Daten zur Verfügung zu stellen, da sie das Vertrauen haben, dass ihre Daten angemessen geschützt sind.

Dieses gesteigerte Vertrauen schafft eine positive Dynamik, in der Beschäftigte und Arbeitgeber gleichermaßen von der Datenverfügbarkeit profitieren können. Die zielgerichtete Nutzung dieser Daten wird dadurch ermöglicht, dass klare und verlässliche Datenschutzregulierungen existieren, die den Schutz der Privatsphäre gewährleisten. Datenschutz wird in diesem Kontext nicht als Hemmnis, sondern als entscheidender Faktor für das Vertrauen und den Erfolg in der datengetriebenen Arbeitswelt wahrgenommen.

Literaturverzeichnis

Acquisti, A./Brandimarte, L./Loewenstein, G. (2015). Privacy and human behavior in the age of information. In: Science, 347(6221), 509–514.

BfDI (2023). FAQ Beschäftigtendatenschutz. ↗ https://www.bfdi.bund.de/DE/Buerger/Inhalte/Arbeit-Besch%C3%A4ftigung/Besch%C3%A4ftigtendaten-schutz/FAQ_Besch%C3%A4ftigtendatenschutz.html [07.12.2023].

Cichy, P./Salge, O./Kohli, R. (2021). Privacy Concerns and Data Sharing in the Internet of Things: Mixed Methods Evidence from Connected Cars. In: MIS Quarterly, 45, 1863–1892.

Datenschutzexperte (2023). Beschäftigtendatenschutz: Alle Fakten zu Datenschutz am Arbeitsplatz. ↗ https://www.datenschutzexperte.de/blog/datenschutz-im-internet/arbeitnehmerdatenschutz/ [11.12.2023].

Martin, N. et al. (2019). How Data Protection Regulation Affects Startup Innovation. In: Information Systems Frontiers, 21(6), 1307–1324.

Meckel, M. (2023). Datensparsamkeit: Deutschland verbaut sich die Zukunft. ↗ https://www.handelsblatt.com/meinung/kolumnen/kolumne-kreative-zerstoerung-datensparsamkeit-deutschland-verbaut-sich-die-zukunft/28980098.html [07.12.2023].

Nanos, A. (2023). Das Eckpunktepapier zum Beschäftigtendatenschutz. ↗ https://www.dids.de/das-eckpunktepapier-zum-beschaeftigtendatenschutz/ [07.12.2023].

Rusch, L. (2023). Beschäftigtendatenschutz. Das könnte das Beschäftigungsdatenschutzgesetz regeln. ↗ https://background.tagesspiegel.de/digitalisierung/das-koennte-das-beschaeftigtendatenschutzgesetz-regeln [07.12.2023].

Schwemmle, M./Wedde, P. (2018). Alles unter Kontrolle? Arbeitspolitik und Arbeitsrecht in digitalen Zeiten. Wiso Diskurs 2, ↗ https://library.fes.de/pdf-files/wiso/14087.pdf [07.12.2023].

Teebken, M. (2023). Privacy and Digital Work: A Conceptualization of Employee Privacy Concerns. epubli.

Teebken, M./Constantiou, I./Hess, T. (2023). Digital Work Versus Privacy? A Conceptual Model on Employee Privacy Challenges. European Conference on Information Systems 2023 (ECIS 2023). ↗ https://www.researchgate.net/publication/372849960_Digital_Work_Versus_Privacy_A_Conceptual_Model_on_Employee_Privacy_Challenges [07.12.2023].

Tolsdorf, J. (2022). Investigation of Information Privacy in Employment: Fundamental Knowledge and Practical Solutions for the Human-Centered Design of Measures to Preserve the Right to Informational Self-Determination in Employment. Dissertation, Georg-August-Universität Göttingen. ↗ https://ediss.uni-goettingen.de/handle/11858/14278 [07.12.2023].

Unabhängige Datenschutzbehörde (2020). Kurzpapier Nummer 14 Beschäftigungsdatenschutz. ↗ https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf [07.12.2023].

Wallace, N./Castro, D. (2018). The Impact of the EU's New Data Protection Regulation on AI. ↗ https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/ [07.12.2023].

Xu, H. et al. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. In: Information Systems Research, 23(4), 1342–1363.

bidt

bidt – Bayerisches Forschungsinstitut
für Digitale Transformation
Gabelsbergerstraße 4
80333 München
↗ www.bidt.digital