R. Reussner, A. Koziolek, R. Heinrich (Hrsg.): INFORMATIK 2020,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2021 815

IT-Rahmenwerk für den Beschäftigtendatenschutz

Technologieeinführung aus rechtlicher und arbeitswissenschaftlicher Perspektive

Christian K. Bosse[1] Aljoscha Dietrich[2] Hartmut Schmitt[3]

Abstract: Die Digitalisierung der Arbeitswelt führt nicht nur zu mehr Flexibilität und Optimierungsmöglichkeiten, sondern ermöglicht auch tiefgreifende Analyse- und Überwachungsmöglichkeiten bezüglich der Arbeitnehmer. Diese Entwicklung kann daher von diesen als Bedrohung empfunden werden und als Reaktion etwa zu Umgehungs- oder Abwehrstrategien führen. Um dieser Problematik zu begegnen, stellen wir in diesem Beitrag ein Rahmenwerk vor, das im Rahmen eines laufenden Forschungsvorhabens erarbeitet wird und das Unternehmen bei der Entwicklung und Einführung IT-gestützter Lösungen für den betrieblichen Datenschutz, z. B. Privacy Dashboards, unterstützen soll. Ausgehend von juristischen und arbeitswissenschaftlichen Aspekten sind wesentliche Bestandteile des Rahmenwerks ein Qualitätsmodell sowie ein Selbstbewertungsinstrument, welches Unternehmen die Einführung entsprechender IT-Lösungen erleichtert.

Keywords: Beschäftigtendatenschutz; Rahmenwerk; Qualitätsmodell; Privacy Enhancing Technolgies; Privacy Dashboards; Selbstbewertung

1 Einleitung und Motivation

Digitalisierte Unternehmen können heute in umfassender Weise die Daten ihrer Arbeitsprozesse erheben und analysieren. Auf dieser Basis optimieren sie Prozesse, etwa indem sie Produktionsabläufe effizienter und kostensparender gestalten. In Zusammenhang mit der digitalen Transformation der Unternehmen werden allerdings immer mehr personenbezogene Daten der Beschäftigten erhoben und verarbeitet, darunter oft Daten, die Rückschlüsse auf Arbeitsverhalten und -leistung, Konsumverhalten oder persönliche Vorlieben zulassen. Dies kann die informationelle Selbstbestimmung der Beschäftigten gefährden und einen unzulässigen Eingriff in die Privatsphäre darstellen, beispielsweise wenn bei der Erfassung von Bewegungsdaten die Grenze zur unzulässigen Überwachung der Beschäftigten überschritten wird [Bo19].

Zwei aktuelle Entwicklungen verdeutlichen die Problematik: Im Personalbereich analysieren immer mehr Unternehmen personenbezogene Daten, um ihre Entscheidungsprozesse zu unterstützen. Mit dieser Praxis – People Analytics genannt – begeben sich die Unternehmen

[1] Institut für Technologie und Arbeit, Trippstadter Str. 113, 67663 Kaiserslautern, christian.bosse@ita-kl.de
[2] Lehrstuhl für Rechtsinformatik, Universität des Saarlandes, 66123 Saarbrücken, aljoscha.dietrich@legalinf.de
[3] HK Business Solutions GmbH, Mellinweg 20, 66280 Sulzbach, hartmut.schmitt@hk-bs.de

doi:10.18420/inf2020_73

in eine rechtliche Grauzone, von manchen Seiten wird sie sogar als rechtswidrig eingeschätzt [Ha20]. Für Aufsehen sorgte Zalando mit einem selbstentwickelten Bewertungssystem [Ze19], aber auch Hersteller wie Microsoft, IBM oder SAP bieten entsprechende Standardprodukte an. Der Home-Office-Boom im Frühjahr 2020, hervorgerufen durch die Corona-Pandemie, veranlasst immer mehr Unternehmen, ihre Mitarbeiter stärker zu überwachen [Mo20]. Dies geschieht durch organisatorische Maßnahmen – Mitarbeiter müssen ihren Vorgesetzten den Zugriff auf E-Mail-Postfächer und Chats gewähren – oder durch Spezialsoftware, die das Mitarbeitertracking ermöglicht. Der Markt solcher Trackingprogramme hat sich innerhalb weniger Wochen verdreifacht [Mo20].

Seit Mai 2018 sorgt die Datenschutzgrundverordnung (DSGVO) für eine strengere Regulierung auch des betrieblichen Datenschutzes: Unternehmen haben erweiterte Informationspflichten gegenüber den Betroffenen, müssen Verarbeitungsverzeichnisse für personenbezogene Daten erstellen und Datenschutzpannen melden. Das Problem: Viele Regelungen der DSGVO sind offen formuliert und machen keine Vorgaben hinsichtlich Technik und Anwendung. Dadurch wissen Unternehmen oft nicht, wie sie sich genau zu verhalten haben, und empfinden die Formulierungen der DSGVO als schwammig [Ma19]. 74 % der Unternehmen sehen einer aktuellen Bitkom-Studie zufolge Datenschutzanforderungen aktuell als größte Hürde beim Einsatz neuer Technologien [Bi19]. Diskutiert wird zudem, inwieweit durch die DSGVO Mitbestimmungsrechte gemäß Betriebsverfassungsgesetz tangiert werden. Durch Urteile und Konkretisierungen in der Praxis müssen also noch einige Lücken geschlossen werden.

Dem Interesse der Unternehmen, die Potentiale einer umfänglichen Datenanalyse zu nutzen, steht das Recht der Betroffenen auf Privatsphäre und informationelle Selbstbestimmung entgegen. Die Betroffenen wissen oft noch nicht einmal, wer welche personenbezogenen Daten zu welchem Zweck verarbeitet und welche Konsequenzen dies für ihre Privatsphäre hat. Ein erfolgversprechender Ansatz, um mögliche Zielkonflikte zwischen Arbeitgebern und Beschäftigten bzw. Mitarbeitervertretungen aufzulösen und eine datenschutzkonforme Verarbeitung personenbezogener Daten zu ermöglichen, sind dedizierte IT-Lösungen für den Beschäftigtendatenschutz. Diese können beispielsweise in Form von Privacy Dashboards ausgestaltet sein. Privacy Dashboards bündeln sämtliche Datenschutzfunktionen in einer zentralen Oberfläche. Sie stellen zum einen Transparenz her, welche personenbezogenen Daten erhoben und verarbeitet werden, denn nur dann sind die Beschäftigten in der Lage, informierte Entscheidungen zu treffen. Zum anderen geben sie den Beschäftigten ein probates Mittel an die Hand, um eigene Datenschutzpräferenzen effektiv durchzusetzen.

Im Forschungsprojekt TrUSD[4] [Tr20] erforschen wir gemeinsam mit weiteren Partnern generische Modelle und Umsetzungskonzepte, aber auch konkrete Ausgestaltungen und Wirkweisen solcher Privacy Dashboards. Die vorgestellten Zwischenergebnisse geben Einblick in dieses laufende Forschungsvorhaben, können aber noch keine Auswertungen des wissenschaftlichen Erfolgs liefern.

[4] Das Forschungsprojekt «TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen» wird gefördert durch das deutsche Bundesministerium für Bildung und Forschung (BMBF).

2 Verwandte Arbeiten

Technische Hilfsmittel, um die Privatsphäre zu schützen bzw. die getätigten Privatsphäre-Einstellungen sicher und zuverlässig durchzusetzen, werden in der Literatur allgemein als *Privacy Enhancing Technologies* (PETs) bezeichnet. Hierbei handelt es sich um eine Vielzahl von Verfahren, wie Anonymisierungsnetze (z. B. TOR) oder Anonymisierungsverfahren in Datenbanken, etwa basierend auf Differential Privacy [Dw06] und k-Anonymität [Sw02]. *Transparency Enhancing Tools* (TETs) hingegen sollen dem Betroffenen die Verarbeitungsprozesse und auch die hieraus entstehenden Konsequenzen erklärbar machen [Fi16]. Privacy Dashboards entsprechen zunächst dem Grundgedanken der TETs indem sie etwa die Verarbeitungsprozesse verdeutlichen, können jedoch auch Funktionalitäten von PETs umfassen. Privacy Insight [BKB16] ist ein Transparenz-Dashboard, das Datenverarbeitungen graphenbasiert anzeigt. Jedoch ist es bisher nicht im industriellen Kontext evaluiert oder für Arbeitnehmer als Nutzer optimiert worden. Es bietet außerdem keine Möglichkeiten zur Selbstbestimmung oder Durchsetzung von Privatheitsbedürfnissen der Nutzer. Die Karlstad-Universität hat mit dem Tool Data Track einen Ansatz vorgestellt, wie die Weitergabe von Daten visualisiert werden kann [Fi16], und die besonderen Anforderungen an Privacy Dashboards in Cloud-Umgebungen erforscht [FAP14]. Allgemeine Anforderungen und eine prototypische Umsetzung wurde von den Telekom Innovation Laboratories in Berlin erforscht [Ra17]. Die TU Berlin arbeitete zusammen mit der Mozilla Corporation an einem benutzerfreundlichen Privacy Dashboard für Firefox OS [Pi15], das Nutzern verschiedene Funktionen von mobilen Endgeräten erklärt, die personenbeziehbare Daten preisgeben, und mit dem die Datennutzung eingeschränkt werden kann. Die Universität Oslo hat ein Identitäts-Dashboard [SJ10] vorgestellt, das Nutzern eine Übersicht über die Verwendung verschiedener digitaler Identitäten und der damit verknüpften Daten gibt. Die Universität Freiburg stellte eine Klassifizierung von Privacy Dashboards [ZAM14] sowie eine empirische Analyse zu deren Akzeptanz [CZM16] vor.

Qualitätsmodelle haben im Software Engineering eine lange Tradition: 1977 nahmen McCall et al. [Mc77] erstmals eine Unterscheidung von Faktoren, Kriterien und Metriken vor, die seitdem als Muster für den Aufbau dieser Modelle dient. Grady & Caswell [GC87] stellten 1987 das Qualitätsmodell FURPS vor, das den Grundstein für den ersten internationalen Standard, ISO 9126, legte. Dessen Revision (ISO 25010) liefert das aktuell umfangreichste Softwarequalitätsmodell. Ein Qualitätsmerkmal Datenschutz fehlt hier allerdings, ebenso relevante Aspekte des strukturellen Umfelds bzw. der Prozesse, in denen ein Softwareprodukt genutzt wird. Von der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wurde als Teil der Modernisierung des Datenschutzrechts ein Konzept von Schutzzielen verabschiedet. Dieses Konzept sowie eine Methode zur Datenschutzberatung und -prüfung wurden 2015 in Form des Standard-Datenschutzmodells (SDM, [AKT19]) veröffentlicht.

Das Konzept der *Selbstbewertung* entstammt ursprünglich dem Bereich des Qualitätsmanagements und findet sich daher auch als durchgängiger Bestandteil der Normreihe ISO 9000

[Ka11]. Im Zuge der Digitalisierung etablierten sich in den letzten Jahren Selbstbewertungsinstrumente als Online-Check. Diese finden sich in den verschiedensten Anwendungsfeldern, in denen sie mit Hilfe von Checklisten und/oder Fragenkatalogen eine Selbstbewertung vor dem Hintergrund eines Reifegradmodells automatisiert vornehmen. Beispiele sind der Online-Check zum Arbeitsschutz der Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege [BGW17] sowie der Readiness-Check Digitalisierung des Mittelstand 4.0-Kompetenzzentrums Kaiserslautern [BH18], dessen ausführliche Dokumentation des Entwicklungs- und Umsetzungsprozesses [HSB19] als Grundlage der Eigenentwicklung im TrUSD-Projekt diente. Ein vergleichbares Selbstbewertungsinstrument, das den Beschäftigtendatenschutz in Unternehmen zum Gegenstand hat, existiert aktuell nicht.

3 Rechtliche Perspektive

Spätestens seit der Anwendung der DSGVO am 25.5.2018 verfügen die Mitgliedstaaten der Europäischen Union über ein einheitliches und verschärftes Datenschutzrecht, das aufgrund der drohenden Sanktionen und Geldbußen bei Verstößen Unternehmen zur Handlung drängt. Ziel der Sanktionen und Geldbußen ist es, wirksam, verhältnismäßig und abschreckend zu sein.[5] Ausdruck hiervon sind mögliche Geldbußen von bis zu 20 Millionen (Mio.) EUR bzw. 4 % des gesamten weltweiten Jahresumsatzes eines Unternehmens. Dass abschreckende Strafen nicht nur in der Theorie bestehen, bewiesen die zuständigen Aufsichtsbehörden bereits am Internetprovider 1&1 (9,4 Mio. EUR), der Immobiliengesellschaft Deutsche Wohnen (14,5 Mio. EUR), der Hotelkette Marriott (ca. 110 Mio. EUR) und British Airways (ca. 204 Mio. EUR) [Ba19a]. Daher ist es schon aus rein betriebswirtschaftlicher Sicht den Unternehmen anzuraten, die Datenschutzgesetzgebung zu befolgen. Motivation braucht jedoch nicht nur Angst vor Strafe sein: ein ernstgenommener Datenschutz kann ebenso ein Wettbewerbsvorteil[6] sein und die Einführung kann zum Aufbau eines Risikomanagements genutzt werden [RCH18].

Die Datenschutzanforderungen bestehen nicht nur nach außen, beispielsweise gegenüber den Kunden, sondern auch innerhalb einer Organisation gegenüber den eigenen Mitarbeitern. Die DSGVO erlaubt für den Beschäftigtendatenschutz explizit nationale Regelungen der Mitgliedsstaaten durch die Öffnungsklausel des Art. 88. In Deutschland wurde hierzu § 26 Bundesdatenschutzgesetz (BDSG) geschaffen. Dieser Paragraph ist jedoch sehr unspezifisch, wie schon § 32 BDSG alter Fassung (a. F.) zuvor. In der Vergangenheit hat dies zu sogenanntem Richterrecht geführt, d. h. Detailregelungen wurden aus hochinstanzlicher Rechtsprechung hergeleitet. Neben fehlender Systematik und Ordnung besteht hierbei eine grundsätzliche Problematik bei der Übertragbarkeit auf andere Fälle. Da sich der Kern des

[5] Vgl. Art. 83 Abs. 1 S. 1 DSGVO sowie [Br19].

[6] Insbesondere wenn von der Möglichkeit der Zertifizierung Gebrauch gemacht wird, vgl. Scholz, Rn. 4, DSGVO Art. 42, in [SHS19].

§ 26 BDSG kaum von seinem Vorgänger unterscheidet, ist jedoch von einer weiteren Anwendbarkeit des Richterrechts auszugehen[7], was wohl auch der Gesetzgeber beabsichtigte.[8] Bestrebungen ein eigenes und detaillierter ausgearbeitetes Beschäftigtendatenschutzgesetz zu schaffen, gibt es seit den 1980er Jahren. Der § 32 BDSG a. F. war ursprünglich ein Provisorium und eine direkte Reaktion auf betriebliche Datenschutzskandale. Die Verabschiedung eines bereichsspezifischen Gesetzes scheiterte jedoch und wurde auf einen Zeitpunkt nach Verabschiedung der DSGVO vertagt.[9]

Eine Analyse der Rechtsprechung zum Mitarbeiterdatenschutz lässt drei Themenschwerpunkte erkennen: Überwachung von Mitarbeitern (insbesondere Videoüberwachung), Einsicht- bzw. Auskunftsrechte sowie Verarbeitung von Mitarbeiterdaten. Die Entscheidungen können herangezogen werden, um Umfang und Grenzen zulässiger Verarbeitung von Mitarbeiterdaten zu bestimmen. Ausgangspunkt ist § 26 Abs. 1 S. 1 BDSG, welcher eine Erforderlichkeit der Verarbeitung von Daten im Beschäftigungsverhältnis voraussetzt. Dies führt zu einer Abwägung zwischen Arbeitgeber- und Arbeitnehmerinteresse. Das Richterrecht hat zu einem dreistufigen Prüfungsschema der Verhältnismäßigkeit geführt, bestehend aus (1) Geeignetheit, (2) Erforderlichkeit und (3) Angemessenheit.[10] Diese Systematik wurde hauptsächlich zu Fragen der Videoüberwachung entwickelt, aufgrund ihrer hohen Abstraktion lässt sie sich jedoch auch gut auf andere Fragestellungen und neuere Technologien übertragen, z. B. Analyse von Nutzungsprotokollen, Kommunikation, Keylogger, Positionsbestimmung oder Wearables. Die Verarbeitungsgrundlage kann im Beschäftigungskontext auch auf Betriebsvereinbarungen fußen, die ebenfalls dem digitalen Wandel unterworfen sind. Vorteile sind u. a. die betriebsweite und grundsätzlich beständige Gültigkeit, im Gegensatz zur Einwilligung [SV20].

Neben den Anforderungen aus § 26 BDSG sind auch die allgemeinen Grundsätze der Verarbeitung (Art. 5 DSGVO) und die Betroffenenrechte (Art. 15–22 DSGVO) umzusetzen, wozu auch die Rechte der Mitarbeiter zählen [Bo19]. Art. 25 Abs. 1 DSGVO verlangt vom Verantwortlichen den Einsatz technischer und organisatorischer Maßnahmen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen. Diese Aufforderung zum technischen Datenschutz findet sich etwas detailreicher wieder in Art. 32 DSGVO – Sicherheit der Verarbeitung. Ein Dashboard für den Beschäftigtendatenschutz kann als eine technische Maßnahme in diesem Sinne bewertet werden. Eine weitere Anforderung für den Verantwortlichen ergibt sich aus Art. 35 DSGVO, der eine Datenschutz-Folgenabschätzung (DSFA) verlangt, wenn eine Verarbeitung erfolgen soll, welche „[...] voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge [...] [hat]“. Zur Identifikation einer solchen Verarbeitung kann ein Verarbeitungsverzeichnis i. S. d. Art. 30 DSGVO hilfreich sein, das vorgeschrieben ist, sofern ein Unternehmen etwa mehr als 250 Mitarbeiter beschäftigt (Art. 30, Abs. 5 DSGVO). Das in Abschnitt 6 vorgestellte

[7] Vgl. hierzu Zöll, BDSG § 26, Rn. 3 in [TG19].
[8] Vgl. [De17], S. 96f.
[9] Vgl. Riesenhuber, § 26, Rn. 8-10, [BW20].
[10] Vgl. hierzu Zöll, BDSG § 26, Rn. 25 in [TG19].

Selbstbewertungsinstrument kann bei der Erstellung eines Verarbeitungsverzeichnisses und Identifizierung der Notwendigkeit einer DSFA unterstützen.

4 Arbeitswissenschaftliche Perspektive

Die Einführung neuer Technologien und digitaler Lösungen bedeutet für Unternehmen einen wichtigen Schritt zur Sicherung ihrer Wettbewerbsfähigkeit. Die Auswertung von Daten, die in den Arbeitsprozessen manuell oder automatisiert verarbeitet werden, bietet die Möglichkeit, bestehende Prozesse und Arbeitsabläufe zu optimieren. Gleichzeitig birgt die Einführung neuer Technologien diverse Risiken in sich. Denn Digitalisierung im Unternehmen bedeutet nicht nur die Einführung einer neuen Technologie, digitalen Lösung oder Software. Sie ist vielmehr ein tiefgreifender Veränderungsprozess, der das gesamte sozio-technische System umfasst [Ul11, Th15]. Viel zu oft wird der Mitarbeiter bzw. die soziale Sphäre im Unternehmen vernachlässigt, sodass von einer Digitalisierung in zwei Geschwindigkeiten gesprochen wird: Einerseits schreitet die technologische Entwicklung rasant voran, während andererseits die erforderliche Gestaltung der Organisationen deutlich mehr Zeit und Veränderungswillen bedarf [Bo19a]. Dabei ist Technologie nur ein Gestaltungselement im Kontext der digitalen Transformation, die neben der technischen Sphäre eines Unternehmens ebenso die organisationale und soziale Sphäre beeinflusst. Die erfolgreiche Einführung digitaler Lösungen ist daher als eine komplexe Gestaltungsaufgabe zu verstehen, deren Wechselwirkungen zwischen allen drei Sphären (Abbildung 1) zu beachten sind [Bo19a].

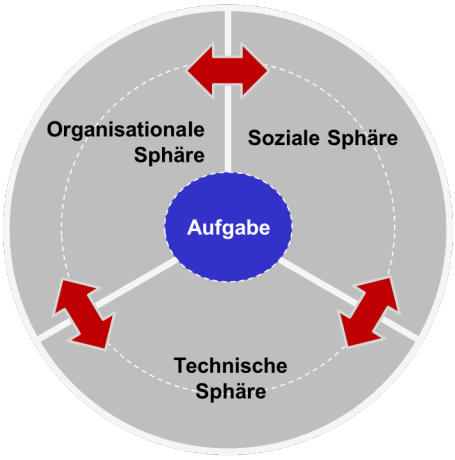

Abb. 1: Wechselwirkung zwischen den drei Sphären der digitalen Transformation als komplexe Gestaltungsaufgabe in Unternehmen

Werden diese komplexen Wirkzusammenhänge nicht ausreichend beachtet, kann es zu Schwierigkeiten bei der Umsetzung kommen. So gilt es bei der Einführung einer neuen Tech-

nologie auf organisationaler Ebene die verschiedenen, kontextspezifischen Regelungen und rechtlichen Vorgaben zu berücksichtigen, wie Gesetze, Normen oder Betriebsvereinbarungen. Gleichzeitig sind die Mitarbeiter einzubeziehen, um eine erfolgreiche Technologieeinführung zu ermöglichen. Die Partizipation bei der Technologieauswahl und -ausgestaltung ist ebenso wichtig wie die Qualifizierung im Hinblick auf die Anwendung. In der Praxis sind viele Szenarien denkbar, in denen ein effizienter Einsatz und das Ausschöpfen des vollen Potenzials einer digitalen Lösung nicht gelingen (können): die ausgewählte Technologie entspricht nicht den Anforderungen am Arbeitsplatz, Mitarbeiter wurden nicht rechtzeitig geschult und sind überfordert oder der Betriebsrat sieht die Mitarbeiter unzulässig überwacht und blockiert den Einsatz der digitalen Lösung [Bo19].

Die komplexen Wirkzusammenhänge zwischen den Sphären sind insbesondere bei der Einführung technischer Lösungen für den Beschäftigtendatenschutz zu beachten. Mit deren Einsatz wird Mitarbeitern die Möglichkeit der Transparenz und Selbstbestimmung bezüglich ihrer personenbezogenen Daten gegeben. Gleichzeitig setzen die Mitarbeiter sich oft erst im Rahmen der Technologieeinführung und -nutzung mit dieser Thematik aktiv auseinander und erfahren bisher unbekannte Details über die Verwendung ihrer personenbezogenen Daten im Unternehmen. Ohne eine vorherige Partizipation der Beschäftigten (soziale Sphäre), eine Anpassung der Prozesse sowie – bei Bedarf – das Abschließen von Betriebsvereinbarungen (organisationale Sphäre) kann dies durch die Mitarbeiter als Überwachung empfunden werden und in nicht intendierte Auswirkungen resultieren. Denkbar ist beispielsweise, dass sich die Beschäftigten ständiger Kontrolle ausgesetzt fühlen und ihr Verhalten derart anpassen, dass es negative Auswirkungen auf sie selbst oder die organisationalen Prozesse und Arbeitsabläufe hat [RS16, DCL15, Pr15]. Des Weiteren kann die Situation in einem gestörten Vertrauensverhältnis zwischen Arbeitgeber und Arbeitnehmer gipfeln, wenn Mitarbeiter versuchen die technische Lösung zu umgehen oder gezielt verfälschte Daten produzieren [Mo15, Pr15]. In der Praxis lassen sich viele Beispiele anführen, z. B. indem Beschäftigte

- bei einer digitalen Zeiterfassung nach dem Ausstechen an den Arbeitsplatz zurückkehren und weiterarbeiten, um hierdurch bestehende Regelungen zu umgehen,
- beim Arbeiten in der Produktion ihre Tätigkeiten bereits als fertig zurückmelden, obwohl nicht alle Tätigkeiten abgeschlossen sind, um so ihre Durchlaufzeiten zu verbessern, oder
- bei einer Videoüberwachung der Eingangsbereiche die Gebäude durch nicht überwachte Notausgänge verlassen, um der Videoüberwachung zu entgehen [Bo19].

Darüber hinaus gibt es Indizien dafür, dass die Überwachung am Arbeitsplatz insgesamt zu einem Verlust der wahrgenommenen Kontrolle und zu einem gesteigerten subjektiven Stresserleben führt [Ba19].

5 Rahmenwerk für den Beschäftigtendatenschutz

Ziel des TrUSD-Projekts ist es, ausgehend von den rechtlichen und arbeitswissenschaftlichen Randbedingungen ein Rahmenwerk zu schaffen, das Unternehmen bei der Entwicklung IT-gestützter Lösungen für den Beschäftigtendatenschutz unterstützt. Da die Unternehmen sich hinsichtlich Größe, Branche, Infrastruktur und Mitarbeiterfähigkeiten unterscheiden, wollen wir möglichst generische, vielseitig einsetzbare Bausteine zur Verfügung zu stellen. Diese sollen den Unternehmen eine geeignete Entscheidungs- und Arbeitsgrundlage bieten, um eine passgenaue Lösung, z. B. ein Privacy Dashboard für ihre Mitarbeiter, zu entwickeln.

In einem Anforderungsmodell haben wir die Bedarfe und Anforderungen der relevanten Stakeholder beschrieben, z. B. Selbstbestimmungs- und Transparenzbedarfe und Benutzer- bzw. Systemanforderungen. Mentale Modelle und Persona-Beschreibungen helfen beim besseren Verständnis der Anwendergruppen, z. B. der Beschäftigten, des Managements oder des Datenschutzbeauftragten. Anwendungsfälle und -szenarien konkretisieren mögliche Einsatzbereiche eines Dashboards, ein Stufenkonzept unterstützt beim schrittweisen Aufbau – vom reinen Informationspanel bis hin zur Transparentmachung von Datenfluss-Manipulationen in Echtzeit [To20]. Ein Architekturkonzept mitsamt integrierten Werkzeugen (z. B. PETs zur Anonymisierung personenbezogener Daten), unterschiedlich gestaltete UI- und Interaktionskonzepte sowie komplementäre Einführungskonzepte helfen außerdem bei der technischen Implementierung und der Einführung im Unternehmen.

5.1 Qualitätsmodell

Ein wesentlicher Bestandteil des Rahmenwerks ist das im Folgenden vorgestellte Qualitätsmodell. Dieses wurde für den Bereich Beschäftigtendatenschutz entwickelt, ist aber auch auf andere Datenschutzbereiche übertragbar. Bei der Entwicklung IT-gestützter Lösungen für den betrieblichen Datenschutz sind unterschiedliche Qualitätseigenschaften von Bedeutung (siehe Abbildung 2). Diese können sich auf die Produktqualität der geplanten Lösung beziehen (z. B. Zuverlässigkeit oder Performanz), aber auch auf deren Nutzungsqualität (z. B. Zufriedenheit der Nutzer), die Prozessqualität (z. B. Prozesskonformität) oder die Strukturqualität (z. B. Kompetenz und Bewusstsein der Mitarbeiter).

Die Grundlage unseres Qualitätsmodells für die Bereiche Produkt- und Nutzungsqualität bildet das Modell der ISO 25010, erweitert um einzelne Teilmerkmale der ISO 9241. Ergänzt wurden außerdem die Gewährleistungsziele des Standard-Datenschutzmodells. Der Bereich Strukturqualität folgt der ISO 9001, der Bereich Prozessqualität dem Modell Gokyo Ri [Kn19]. Bei der Integration des Qualitätsmodells in das Rahmenwerk gilt unser besonderes Augenmerk den Beziehungen zwischen einzelnen Qualitätseigenschaften (vgl. [Wa02]). Es ist ersichtlich, welche Eigenschaften sich verstärken, z. B. Korrektheit und Zuverlässigkeit, und welche Eigenschaften miteinander konkurrieren, d. h., eine Maßnahme zur Verbesserung der einen Eigenschaft führt potentiell zu einer Verschlechterung der anderen Eigenschaft, z. B. Verfügbarkeit und Vertraulichkeit.

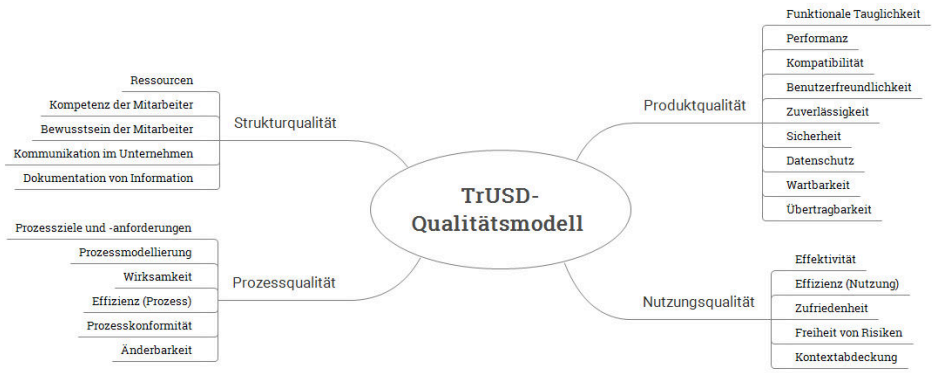

Abb. 2: Übersicht des Qualitätsmodells für den Beschäftigtendatenschutz

5.2 Operationalisierung

Damit Anwender des Rahmenwerks potentielle Konflikte identifizieren und einen geeigneten Trade-off ermitteln können, haben wir die Qualitätseigenschaften jeweils mit typischen Umsetzungsmaßnahmen verknüpft (Beispiel: „Integrität“ ist verknüpft mit „Schutz vor Schadsoftware“). Hierbei haben wir sowohl die verstärkenden als auch die konkurrierenden Beziehungen im Rahmenwerk dokumentiert. Zudem haben wir bei den Qualitätseigenschaften jeweils Checklistenpunkte hinterlegt. Diese helfen zum einen beim Erreichen bestimmter Qualitätseigenschaften, zum anderen ermöglichen sie im Nachgang eine systematische Bewertung der entwickelten Lösung. Auf Grundlage dieses Rahmenwerks entwickeln mehrere Partner des TrUSD-Projekts exemplarische Lösungen, die mit Endanwendern getestet und evaluiert werden. Hierbei wird untersucht, ob die Dashboards mehr Transparenz bei der Erhebung und Nutzung personenbezogener Daten im Unternehmen schaffen, die Durchsetzung eigener Datenschutzpräferenzen ermöglichen und so zu einem fairen Ausgleich zwischen Arbeitgeber- und Arbeitnehmerinteressen beitragen.

6 Betriebsinterne Feststellung des Datenschutzniveaus

Die Umsetzung rechtlicher Vorgaben stellt insbesondere kleine und mittlere Unternehmen vor eine Herausforderung, die oft nur mit externer Unterstützung zu schaffen ist. Denn zumeist verfügen diese Unternehmen nicht über das notwendige Fachwissen, um die in juristischer Fachsprache verfassten rechtlichen Verordnungen zu verstehen und einen rechtskonformen Datenschutz umzusetzen. Gleichzeitig führen die potenziellen Strafen in vielen Unternehmen zu großen Unsicherheiten [Be19]. Selbst wenn einzelne Maßnahmen bereits ergriffen wurden, bestehen oft unbedachte, bis dato unbekannte Lücken im Datenschutz, verdeutlicht an folgendem Beispiel: Um Auswertungen der elektronisch erfassten Arbeitszeiten zu

verhindern, die über die Lohnabrechnung hinausgehen und Rückschlüsse über die Effizienz der einzelnen Mitarbeiter zulassen, werden die Daten und die Auswertungsfunktion der Zeiterfassungssoftware mit einer Zugriffskontrolle versehen. Lediglich die Personalabteilung kann einsehen, welcher Mitarbeiter zu welcher Uhrzeit ein- bzw. ausgestochen hat. Auf den ersten Blick sind somit die personenbezogenen Daten über die individuellen Arbeitszeiten geschützt. Die zentrale Stechuhr befindet sich jedoch im Eingangsbereich des Gebäudes, der mit einem elektronischen Schließsystem gegen Fremdzutritt gesichert und videoüberwacht ist. Somit ist es Dritten (z. B. dem Sicherheitsdienst) möglich, anhand der vom Schließsystem erfassten Daten oder der Auswertung der Videoaufnahmen die Arbeitszeiten der Mitarbeiter zu eruieren. Während die Auswertung von Videomaterial aus Überwachungskameras meist in Betriebsvereinbarungen geregelt ist, werden die Erfassungsdaten eines elektronischen Schließsystems oft nicht bedacht.

Um den Ist-Zustand des Datenschutzes im Unternehmen ohne großen Ressourcenbedarf oder Unterstützung externer Berater zu ermitteln, bietet sich der Einsatz eines Selbstbewertungsinstruments an. Diese Instrumente erfreuen sich in den letzten Jahren großer Beliebtheit und werden von Unternehmen beispielsweise zur Ermittlung des digitalen Reifegrades [BH18] oder zur Einschätzung der Organisation des Arbeitsschutzes [BGW17] eingesetzt. Dabei werden meist nicht nur die Ergebnisse der Selbstbewertung dokumentiert, sondern auch Entwicklungspotenziale aufgezeigt und Lösungen aus Expertensicht vorgeschlagen [HSZ18]. Ein solches Selbstbewertungsinstrument, das den Beschäftigtendatenschutz in Organisationen und Unternehmen zum Gegenstand hat, entwickeln und erproben wir im Rahmen des TrUSD-Projekts. Ziel des Instruments ist es zum einen, Organisationen und Unternehmen für das Thema Datenschutz zu sensibilisieren. Zum anderen wird Geschäftsführern, Führungskräften und weiteren Verantwortliche eine praxisgerechte Unterstützung bei der (Weiter-)Entwicklung eines unternehmensspezifischen und rechtskonformen Datenschutzes zur Verfügung gestellt.

Um die Entwicklung anzugehen, haben wir zunächst Online-Selbstbewertungsinstrumente aus anderen Themenbereichen analysiert. Grundlage für die Entwicklung unseres Instruments bildet ein Kriterienkatalog, der eine systematische Erfassung des Ist-Zustands und eine Bewertung der Umsetzung datenschutzrechtlicher Anforderungen ermöglicht. Dieser Kriterienkatalog basiert zum einen auf den Ergebnissen der Projektarbeit, beispielsweise der Anforderungserhebung bei den Anwendungspartnern, den erhobenen Datennutzungs- und Schutzbedarfen sowie den Selbstbestimmungs- und Transparenzbedarfen. Zum anderen referenzieren wir die Anforderungen der DSGVO sowie die Gewährleistungsziele des Standard-Datenschutzmodells: Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit und Evaluierbarkeit. Das Selbstbewertungsinstrument ist außerdem eng verbunden mit dem Verarbeitungsverzeichnis des Art. 30 DSGVO, in dem alle Verarbeitungstätigkeiten in der Zuständigkeit des Verantwortlichen zu erfassen sind. Besteht ein Verarbeitungsverzeichnis, kann es genutzt werden, um die Fragen schneller zu beantworten. Besteht es nicht, kann das Selbstbewertungsinstrument bei dessen Erstellung unterstützen. Folgend kann dies bei der Identifizierung von Verarbeitungsvorgän-

gen genutzt werden, welche voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Beschäftigten darstellen und daher eine Datenschutz-Folgenabschätzung i. S. d. Art. 35 DSGVO bedürfen. Ergänzend werden weiche Faktoren adressiert, die ebenfalls ein wichtiger Bestandteil des Datenschutzes in Organisationen sind [Wa12], zum Beispiel die Information, Sensibilisierung und Qualifizierung der Mitarbeiter. Ziel des Selbstbewertungsinstruments ist es, eine möglichst vollständige und umfassende Abdeckung der verschiedenen Facetten des Beschäftigtendatenschutzes sowie eine allgemeine Verständlichkeit auch für juristische Laien zu erreichen.

Das Selbstbewertungsinstrument haben wir als Online-Befragung mit der Open-Source-Software LimeSurvey umgesetzt. Mit Hilfe eines für Laien gut verständlichen Fragenkatalogs, der auf dem umfassenden Kriterienkatalog basiert, werden sowohl rechtliche als auch arbeitswissenschaftliche Aspekte erhoben. Die Online-Befragung wird dabei in verschiedene Themenbereiche strukturiert, um sie übersichtlicher zu gestalten. Darüber hinaus wird die Anzahl der zu beantwortenden Fragen durch den Einsatz von Filterfragen optimiert, sodass gegebenenfalls im Unternehmenskontext irrelevante Fragen nicht angezeigt werden. Auf diese Weise wird das Verhältnis von Aufwand zu Nutzen bei Einsatz des Selbstbewertungsinstruments unternehmensindividuell optimiert.

Insgesamt bietet das Selbstbewertungsinstrument die Möglichkeit, den Ist-Zustand des Beschäftigtendatenschutzes zu erheben. Dies geschieht durch eine auf den gegebenen Antworten basierende Einschätzungen zur Rechtskonformität und zum Reifegrad im Bereich des Beschäftigtendatenschutzes bzgl. der bisher umgesetzten Maßnahmen. Jeder Teilnehmer erhält unmittelbar die Auswertung seiner individuellen Ergebnisse und daran anknüpfende Handlungsempfehlungen zur Weiterentwicklung des Beschäftigtendatenschutzes. Zudem stehen Checklisten bereit, mit deren Hilfe die rechtskonforme Umsetzung im Unternehmen gefördert wird. Dieses Selbstbewertungsinstrument wird nach Abschluss der Test- und Evaluationsphase online frei zur Verfügung stehen.

7 Fazit

Durch die Digitalisierung und die Anwendbarkeit der DSGVO sind Unternehmen vor neue Herausforderungen im Beschäftigtendatenschutz gestellt. Geeignete IT-Lösungen, beispielsweise in Form von Privacy Dashboards, unterstützen Unternehmen bei einer rechtskonformen Umsetzung des Beschäftigtendatenschutzes. Die verbesserte Transparenz und Mitbestimmung erzeugen bei den Mitarbeitern zudem eine höhere Akzeptanz der Datenverarbeitung. Besonders relevant für eine erfolgreiche Umsetzung sind eine umfassende und möglichst vollständige Anforderungserhebung und das hieraus abgeleitete Qualitätsmodell, beides Bestandteile des vorgestellten Rahmenwerks. Ein komplementäres Selbstbewertungsinstrument unterstützt Unternehmen bei der Analyse des Ist-Zustands sowie bei der Implementierung und Evaluation technischer bzw. organisationaler Lösungen.

Literaturverzeichnis

[AKT19] AK Technik, DSK: Das Standard-Datenschutzmodell, Version 2.0. Beschluss der 98. DSK, Trier, 2019.

[Ba19] Backhaus, N.: Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz. Zeitschrift für Arbeitswissenschaft, Vol. 73 Iss. 1, S. 2-22, 2019.

[Ba19a] Bayrischer Rundfunk: Datenschutzgrundverordnung: Die Schonfrist ist vorbei, https://www.br.de/nachrichten/bayern/datenschutzgrundverordnung-die-schonfrist-ist-vorbei, Stand: 29.4.2020.

[Be19] Becker, W. et.al.: Digitale Arbeitswelten im Mittelstand. Veränderungen und Herausforderungen. Springer, Wiesbaden, 2019.

[BGW17] BGW, Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege: Online-Check zum Arbeitsschutz. Heilberufe, vol. 69, iss. 7-8, S. 41, 2017.

[BH18] Bosse, C. K.; Hellge, V.: Digitalisierung im Mittelstand. Zeitschrift für Organisationsentwicklung, 01/18, S. 102-103, 2018.

[BKB16] Bier, C. et al.: PrivacyInsight: The Next Generation Privacy Dashboard. 4th Annual Privacy Forum, APF, Frankfurt a.M. September 7-8, 2016.

[Bi19] Bitkom e.V. (2019). Bitkom zieht gemischte Jahresbilanz zur DS-GVO `https://www.bitkom.org/Presse/Presseinformation/Bitkom-zieht-gemischte-Jahresbilanz-zur-DS-GVO`, Stand: 29.4.2020.

[Bo19] Bosse, C. K. et.al.: Beschäftigtendatenschutz: Rechtliche Anforderungen und technische Lösungskonzepte. In (Schweighofer, E.; Kummer, F.; Saarenpää, A., Hrsg.): Tagungsband des 22. Internationalen Rechtsinformatik Symposions (IRIS), 2019.

[Bo19a] Bosse, C. K. et.al.: Digitalisierung im Mittelstand erfolgreich gestalten. In (Bosse, C.K.; Zink, K.J., Hrsg.): Arbeit 4.0 im Mittelstand. Chancen und Herausforderungen des digitalen Wandels für KMU. Springer, Berlin/ Heidelberg, 2019.

[Br19] Brink, S.: Bußgeldrahmen nach der DS-GVO, ZD 2019, 141.

[BW20] Brink, S; Wolff, A.: BeckOK Datenschutzrecht, 32. Edition, 1.5.2020, C.H. Beck, 2020.

[Cr12] Cranor, L. F.: „P3P is dead, long live P3P!, http://lorrie.cranor.org/blog/2012/12/03/p3p-is-dead-long-live-p3p/, Stand: 29.4.2020.

[DCL15] Da Cunha, J. V.; Carugati, A.; Leclercq-Vandelannoitte, A.: The dark side of computer-mediated control. Information Systems Journal, 25, S. 319-354, 2015.

[CZM16] Cabinakova, J.; Zimmermann, C.; Mueller, G.: An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case. ECIS, Istanbul, Turkey, June 12-15, 2016.

[De17] Deutscher Bundestag: Drucksache 18/11325, 2017.

[Dw06] Dwork, C.: Differential Privacy, in: Automata, Languages and Programming: 33rd ICALP 2006, LNCS, Bd. 4052, S. 1-12, Springer, Berlin/Heidelberg, 2006.

[FAP14] Fischer-Hübner, S. et al.: How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?, in Privacy and Identity Management for Emerging Services and Technologies, S. 77–92. Springer Berlin/Heidelberg, 2014.

[Fi16] Fischer-Hübner, S. et al.: Transparency, Privacy and Trust – Technology for Tracking and Controlling My Data Disclosures: Does This Work?. 10th IFIP TM, Jul 2016, Darmstadt, Germany. pp.3-14

[GC87] Grady, R. B.; Caswell, D. L.: Software Metrics: Establishing a Company-Wide Program. Prentice-Hall, Englewood Cliffs, N.J., 1987.

[Ha20] Hagelüken, A.: Arbeitswelt – Personalanalyse von Mitarbeitern oft rechtswidrig. In: Süddeutsche Zeitung vom 02.03.2020. München: Süddeutsche Zeitung.

[HSB19] Hellge, V.; Schröder, D.; Bosse, C.K.: Der Readiness-Check Digitalisierung. Ein Instrument zur Bestimmung der digitalen Reife von KMU. Mittelstand 4.0-Kompetenzzentrum Kaiserslautern. https://kompetenzzentrum-kaiserslautern.digital/wp-content/uploads/2019/01/Broschüre_Readiness_Check_Digitalisierung_Januar_2019_final.pdf

[HSZ18] Hellge, V.; Schröder, D.; Zink, K.J.: Der Readiness-Check „Digitalisierung“ als Instrument im digitalen Transformationsprozess. In (Lingnau, V.; Müller-Seitz, G.; Roth, S., Hrsg.): Management der digitalen Transformation. Vahlen, 2019.

[Ka11] Kamiske, G.F.; Brauer, J.-P.: Qualitätsmanagement von A-Z. Hanser, 2011.

[Kn19] Kneuper, R.: Messung und Bewertung von Prozessqualität mit Gokyo Ri. http://www.kneuper.de/GokyoRi/, Stand: 29.4.2020.

[Ma19] Martin-Jung, H.: Datenschutzgrundverordnung – Das verflixte erste Jahr. In: Süddeutsche Zeitung vom 25.05.2019. München, Süddeutsche Zeitung.

[Mc77] McCall, J. A.; Richards, P. K.; Walters, G. F.: Factors in Software Quality. US Rome Air Development Center Reports I-III. U.S. Department of Commerce, Washington, 1977.

[Mo15] Mohammad, M.: IT Surveillance and Social Implications in the Workplace. Proceedings of the 2015 SIGMIS Conference on Computers and People Research, 2015.

[Mo20] Moorstedt, M.: https://www.sueddeutsche.de/digital/home-office-ueberwachung-tracking-chef-zoom-1.4868739, SZ, 2020, Stand: 29.4.2020.

[Pi15] Piekarska, M. et.al.: Because we care: Privacy Dashboard on Firefox OS. In: Proceedings of the 9th Workshop on Web 2.0 Security and Privacy, 2015.

[Pr15] Pritchard, G. W. et.al.: How to Drive a London Bus: Measuring Performance in a Mobile and Remote Workplace, 33rd ACM CHI ’15, S. 907-916, 2015.

[Ra17] Raschke, P. et.al.: Designing a GDPR-compliant and usable privacy dashboard. In: IFIP International Summer School on Privacy and Identity Management, S. 221-236. Springer, Cham, 2017.

[RCA19] Reiserer, K.; Christ, F.; Heinz, K.: Beschäftigtendatenschutz und EU-Datenschutz-Grundverordnung, DStrR 2018, 1501.

[RS16] Rosenblatt, A.; Stark, L.: Algorithmic Labor and Information Asymmetries: A Case Study of Uber’s Drivers. Int. Journal of Communication, 16, S. 3758–3784, 2016.

[SHS19] Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I.: Datenschutzrecht, NOMOS, 2019

[SJ10] Scudder, J.; Jøsang, A.: Personal Federation Control with the Identity Dashboard. Policies and Research in Identity Management, IDMAN 2010, Oslo, November 18-19, 2010.

[SV20] Schulze, M.; Volk, T.: Die Anpassung von Betriebsvereinbarungen an die Betriebswirklichkeit, ArbR Aktuell 2020, 60.

[Sw02] Sweeney, L.: k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, Vol 10, Issue 5, 2002, S. 557-570.

[TG19] Taeger, J.; Gabel, D.: Kommentar DSGVO – BDSG. Deutscher Fachverlag GmbH, Frankfurt a.M., 3. Auflage, 2019.

[Th15] Thul, M. J.: Der sozio-technische Systemansatz. In (Zink, K. J. et al., Hrsg.): Veränderungsprozesse erfolgreich gestalten, 2. Aufl., Springer Vieweg, S. 278-283, 2015.

[To20] Tolsdorf, J. et.al.: Privatheit am Arbeitsplatz. DuD, Vol. 44, Nr. 3, S. 176-181, 2020.

[Tr20] TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen. https://www.trusd-projekt.de, Stand: 29.4.2020.

[Ul11] Ulich, E.: Arbeitspsychologie, 7. Auflage, Schäffel-Poeschel Verlag, 2011.

[W3C06] W3C, „The Platform for Privacy Preferences 1.1 (P3P1.1) Specification“, W3C Working Group Note, Nov. 2006.

[Wa02] Wallmüller, E.: Qualitätsmodelle im Software Engineering. In: MQ - Management und Qualität 2002(9). Galledia Verlag, Berneck, 2002.

[Wa12] Wagner, E.: Datenschutz als Bildungsauftrag. DuD, 02/12, S. 83-87, 2012.

[ZAM14] Zimmermann, C.; Accorsi, R.; Muller, G.: Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy, ARES 2014, 2014, S. 152–157.

[Ze19] Zeit Online (2019): Zonar: Datenschutzbehörde prüft Mitarbeitersoftware von Zalando. URL: https://www.zeit.de/arbeit/2019-11/zonar-zalando-mitarbeiter-scoring-software, Stand: 29.4.2020.