BESCHÄFTIGTENDATENSCHUTZ: RECHTLICHE ANFORDERUNGEN UND TECHNISCHE LÖSUNGSKONZEPTE

Christian K. Bosse / Aljoscha Dietrich / Patricia Kelbert / Hagen Küchler / Hartmut Schmitt / Jan Tolsdorf / Andreas Weßner

Wissenschaftlicher Mitarbeiter, Institut für Technologie und Arbeit, Trippstadter Str. 113, 67663 Kaiserslautern, DE, christian.bosse@ita-kl.de, https://ita-kl.de

Wissenschaftlicher Mitarbeiter, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes, 66123 Saarbrücken, DE, aljoscha.dietrich@uni-saarland.de, https://www.legalinf.de

Wissenschaftliche Mitarbeiterin, Fraunhofer IESE, Security Engineering, Fraunhofer-Platz 1, 67663 Kaiserslautern, DE, patricia.kelbert@iese.fraunhofer.de, https://www.iese.fraunhofer.de/de/competencies/security.html

Studentischer Mitarbeiter, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes 66123 Saarbrücken, DE, hagen.kuechler@uni-saarland.de, https://www.legalinf.de

Projektleiter, HK Business Solutions GmbH, Mellinweg 20, 66280 Sulzbach, DE, hartmut.schmitt@hk-bs.de, http://www.hk-bs.de

Wissenschaftlicher Mitarbeiter, Data & Application Security Group, Technische Hochschule Köln, 50679 Köln, jan.tolsdorf@th-koeln.de, https://das.th-koeln.de

Wissenschaftlicher Mitarbeiter, Institut für Technologie und Arbeit, Trippstadter Str. 113, 67663 Kaiserslautern, DE, andreas.wessner@ita-kl.de, https://ita-kl.de

Schlagworte: ***DSGVO, Beschäftigtendatenschutz, Technische Lösungen, Privatheit, Transparenz, Selbstbestimmung, digitale Transformation***

Abstract: *Die Digitalisierung betrifft nahezu alle Bereiche der Gesellschaft und somit auch die Beschäftigten. Neben wirtschaftlichen Potenzialen hat diese Entwicklung auch bisher unbekannte Überwachungsmöglichkeiten zur Folge. Da die Datenschutzgesetze in Deutschland nur sehr unspezifische Vorgaben für den Beschäftigtendatenschutz machen, ist es erforderlich, diese aus Rechtsprechung und datenschutzrechtlichen Grundsätzen abzuleiten. Auf dieser Grundlage werden technische Lösungsvorschläge vorgestellt, die den Beschäftigten als Werkzeug für Transparenz und Kontrolle über die Verwendung ihrer Daten dienen können.*

1. Einführung und Motivation

Die heutige Gesellschaft und Wirtschaft sind geprägt durch digitale Geräte und digitale Technologien. Einst analoge Informationen werden in digitale Formate umgewandelt, für physische Objekte und Ereignisse werden digitale Repräsentationen erstellt. Als Folge dieser digitalen Transformation können Daten aus nahezu allen Lebens- und Arbeitsbereichen informationstechnisch verarbeitet und in vielfältiger Weise genutzt werden. In der Arbeitswelt betrifft dieser Trend längst nicht mehr nur klassische IT-Unternehmen, sondern sämtliche Branchen und Sektoren.[1] Klassische Arbeitsplätze verändern sich, Unternehmensprozesse werden neu ausgerichtet, innovative digitale Geschäftsmodelle entstehen. In der industriellen Produktion kommt es durch

[1] Bundesministerium für Wirtschaft und Energie, Den digitalen Wandel gestalten https://www.bmwi.de/Redaktion/DE/Dossier/digitalisierung.html (aufgerufen am 30. Oktober 2019), 2019.

digitale Innovationen oft zu einem radikalen Wandel, auch digitale Disruption genannt. Entsprechend bezeichnet man das Phänomen «Digitalisierung» hier auch als vierte industrielle Revolution oder Industrie 4.0.[2]

Durch die Digitalisierung haben Unternehmen heute erstmals die Möglichkeit, in umfassender Weise Daten ihrer Arbeitsprozesse zu erheben und zu analysieren. Auf dieser Basis können Entscheidungsträger Prozesse optimieren, etwa indem sie Produktionsabläufe effizienter und kostensparender gestalten; allerdings werden hierbei auch immer mehr personenbezogene Daten der Arbeitnehmer erhoben und verarbeitet.[3] Dies kann die informationelle Selbstbestimmung der Arbeitnehmer gefährden und einen unzulässigen Eingriff in deren Privatheit bedeuten, beispielsweise wenn die Grenze zur unzulässigen Überwachung überschritten wird. Ein Praxisbeispiel veranschaulicht dies: In einem Lager werden die Bewegungsdaten von Arbeitnehmern genutzt, um ineffiziente Abläufe aufzudecken und das Lager besser zu organisieren. Zur Aufdeckung unnötiger Wege reicht eine Analyse anonymisierter Bewegungsdaten aus. Die Arbeitnehmer selbst können jedoch nicht sicherstellen, dass ihre Bewegungsdaten nicht auch zur Erstellung unzulässiger Bewegungsprofile genutzt werden, einschließlich des Verhaltens in den Arbeitspausen und über die Grenzen des Betriebsgeländes hinaus. Der Arbeitgeber muss also mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass keine direkte Überwachung einzelner Arbeitnehmer stattfindet. Neue Technologien, z. B. Wearables, verschaffen Unternehmen bisher ungeahnte Möglichkeiten, personenbezogene Daten ihrer Mitarbeiter zu verarbeiten. Wearables sind kleine Computersysteme, die am Körper getragen werden und mit denen z. B. Geo-Position, Körperaktivitäten oder Herzfrequenz des Trägers erhoben werden können. Der Arbeitgeber ist dadurch in der Lage, Korrelationen zwischen Aktivitäts- und Ruhezuständen sowie Arbeitseffizienz herzustellen[4] und aus Bewegungsmustern Anzeichen auf Krankheiten und Behinderungen abzuleiten.[5]

Bereits jetzt verfügen Arbeitnehmer meist weder über das Wissen noch die Möglichkeit, die über sie erhobenen personenbezogenen Daten, deren Verarbeitung und die damit verbundenen Konsequenzen für ihre Privatheit zu verstehen, geschweige denn zu kontrollieren. Es gilt also, mehr Transparenz zu schaffen und einen fairen Ausgleich zwischen den Interessen der Arbeitgeber und der Arbeitnehmer bzw. der Arbeitnehmervertretungen, z. B. Betriebs- und Personalräten, herbeizuführen. Hierzu bedarf es praxistauglicher und rechtskonformer Lösungen, welche die Transparenz- und Schutzziele der Arbeitnehmer und die Interessen der Arbeitgeber an einer Datennutzung miteinander in Einklang bringen: Arbeitnehmer benötigen verständliche Informationen, welche personenbezogenen Daten von wem und zu welchem Zweck verarbeitet bzw. geteilt werden. Nur dann sind sie in der Lage, informierte Entscheidungen zu treffen, die die eigene Privatsphäre am Arbeitsplatz betreffen – also beispielsweise, ob bestimmte Daten nur anonymisiert verwendet werden sollen. Zudem müssen ihnen Mittel an die Hand gegeben werden, mit denen sie die eigenen Datenschutzpräferenzen ausdrücken und wirksam durchsetzen können. Gleichzeitig können Arbeitgeber, die in ihrem Unternehmen die datenschutzkonforme Verarbeitung der personenbezogenen Daten sicherstellen, die Potenziale einer umfänglichen Datenanalyse nutzen, ohne sich in einer rechtlichen Grauzone zu bewegen. Durch mehr Transparenz beim Umgang mit Mitarbeiterdaten können sie zudem von einer Stärkung der Vertrauens- und Arbeitskultur in ihrem Unternehmen profitieren.

---

2 Bendel, Oliver, Digitalisierung. In: Gabler Wirtschaftslexikon. https://wirtschaftslexikon.gabler.de/definition/digitalisierung-54195/version-277247 (aufgerufen am 30. Oktober 2019), 2018.

3 Heckmann, Dirk, Studie: Daten als Wirtschaftsgut. https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2018/Downloads/Studie-Daten-als-Wirtschaftsgut_final.pdf (aufgerufen am 30. Oktober 2019), 2018.

4 Dietrich, Aljoscha/Krüger, Jochen/Potel, Karin, Wearables im Zugriff der Strafjustiz. In: Erich Schweighofer et al., (Hrsg.), Trends und Communities der Rechtsinformatik: Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017, Wien 2017, S. 561–568.

5 Sung, Michael/Marci, Carl/Pentland, Alex, Wearable feedback systems for rehabilitation. In: Journal of NeuroEngineering and Rehabilitation 2.17, 2005.

2. Rechtliche Anforderungen

Der Beschäftigtendatenschutz in Deutschland, auch Arbeitnehmerdatenschutz genannt, ist ein eher junges Rechtsgebiet. Aufgrund fehlender eigener Regelungen erfolgte anfänglich noch ein Rückgriff auf Grundgesetz und das Betriebsverfassungsgesetz. Das Bundesdatenschutzgesetz (BDSG), welches 1978 in Kraft trat, enthielt noch keine spezifischen Regelungen zum Arbeitnehmerdatenschutz.[6] Erst nach Bekanntwerden der Überwachungsaffären von Deutscher Telekom[7] und Lidl[8] im Jahr 2008 wurde das BDSG 2009 um § 32 (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses) ergänzt. Weitere Versuche des Gesetzgebers eine differenziertere Ausgestaltung des Arbeitnehmerdatenschutzes zu schaffen waren nicht erfolgreich und wurden wegen der in Aussicht stehenden Europäischen Datenschutz-Grundverordnung (DSGVO) nicht weiter verfolgt.[9] Aufgrund der unspezifischen Regelungen wurden viele Fragen bzgl. des Arbeitnehmerdatenschutzes von Gerichten geklärt und haben zu einem sogenannten Richterrecht geführt.[10] Die Entscheidungen sind allerdings weder systematisch noch übersichtlich geordnet, auch eine Übertragung auf andere Fälle ist eingeschränkt, da lediglich Aussagen zu sehr spezifischen Fragestellungen getroffen wurden.

Am 25. Mai 2018 trat neben der DSGVO auch das BDSG n. F. (neue Fassung) in Kraft. Das BDSG n. F. stellt die deutsche Ausgestaltung des Datenschutzes dar und greift hierfür auf die Öffnungsklauseln der DSGVO zurück. § 26 BDSG n. F. füllt die Öffnungsklausel des Art. 88 DSGVO aus, welche nationale Regelungen für die Datenverarbeitung im Beschäftigungskontext erlaubt.[11] Da § 32 BDSG a. F. weitestgehend wortgleich übernommen wurde, können wohl auch weiterhin die entwickelten Auslegungsgrundsätze und die Rechtsprechung (Richterrecht) herangezogen werden.[12] Der Gesetzgeber entschied sich bewusst gegen eine größere und spezifischere Neuregelung, da einschlägige Rechtsprechung des EuGH erwartet wird.[13]

§ 26 BDSG n. F. beschreibt vier Erlaubnistatbestände für die Verarbeitung von Beschäftigtendaten:

1. die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses, § 26 I S. 1 BDSG n. F.,
2. die Verarbeitung von Beschäftigtendaten, soweit es der Aufdeckung von Straftaten dient, § 26 I S. 2 BDSG n. F.,
3. die Kollektivvereinbarung, § 26 I S. 1, IV BDSG n. F., sowie
4. die Einwilligung, § 26 II BDSG n. F.

Die Erlaubnistatbestände teilen sich denselben persönlichen und sachlichen Anwendungsbereich. Der persönliche Anwendungsbereich umfasst alle Beschäftigten, welche in § 26 VIII BDSG n. F. definiert werden. Zur Erfüllung des sachlichen Anwendungsbereichs, müssen drei Merkmale vorliegen: (1) Personenbezogene Daten, (2) Verarbeitung und (3) Zweck des Beschäftigungsverhältnisses. Die Definitionen der Merkmale (1) und (2) finden sich in der DSGVO.[14] In § 26 I S. 1 BDSG n. F. findet sich eine Erläuterung für Merkmal (3), welches alle Daten umfasst, die für Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses

---

6 Riesenhuber, Dirk, § 26 BDSG, Rn. 6. In: BeckOK Datenschutzrecht, Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), 29. Edition, Stand: 01.08.2019.

7 Leyendecker, Hans, Die Macht des Geldes. Süddeutsche Zeitung, 27. Mai 2008, aufgerufen am 30. Oktober 2019.

8 Der Spiegel, Lidl ließ Mitarbeiter systematisch bespitzeln, 26.03.2008, abgerufen am 25.10.2019.

9 Stamer, Katrin/Kuhnke, Michael, § 26 BDSG Rn. 1. In: DSGVO/BDSG, Plath, Kai-Uwe (Hrsg.), Otto Schmidt, 3. Auflage, 2018.

10 Ströbel, Lukas/Wybitul, Tim, §10 Beschäftigtendatenschutz, Rn. 2. In: Handbuch Europäisches und deutsches Datenschutzrecht, Specht, Louisa/Mantz, Reto (Hrsg.), C.H. Beck, 2019.

11 Riesenhuber, § 26 BDSG, Rn. 5; Kühling, Jürgen, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, S. 1985.

12 Gräber, Tobias/Nolden, Christine, § 26 BDSG, Rn. 2. In: DS-GVO BDSG, Paal, Boris P./Pauly, Daniel A. (Hrsg.), C.H. Beck, 2. Auflage, 2018.

13 BT-Drs. 18/11325, S.97; Kühling, Jürgen/Klar, Manuel/Sackmann, Florian, Datenschutzrecht, C.F. Müller, 4. Auflage, Rn. 800; Maschmann, Frank, § 26 BDSG, Rn. 2. In: Datenschutz-Grundverordnung, Kühling, Jürgen/Buchner, Benedikt (Hrsg.), C.H. Beck, 2. Auflage, 2018.

14 «Personenbezogene Daten» sind in Art. 4 Nr. 1 DSGVO, «Verarbeitung» ist in Art. 4 Nr. 2 DSGVO definiert.

notwendig sind.[15] Diese personenbezogenen Mitarbeiterdaten umfassen unter anderem Name, Adresse, Alter, Familienstand und Nationalität.[16] Sie werden gemeinhin unter dem Begriff «Stammdaten» zusammengefasst und dürfen grundsätzlich im Beschäftigungskontext verarbeitet werden. Zu beachten ist jedoch, dass der Begriff der Stammdaten ausschließlich durch die Literatur und Rechtsprechung ausgeformt wurden. Auch gilt es, die Zweckbindung der Beschäftigtendaten[17] sowie die Erforderlichkeit der Verarbeitung zu beachten. Die Erforderlichkeit bemisst sich nach der Verhältnismäßigkeit. In der Gesetzesbegründung des «Datenschutz-Anpassungs- und -Umsetzungsgesetz EU» heißt es hierzu, dass «die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem Ausgleich gebracht werden [sollen], der beide Interessen möglichst weitgehend berücksichtigt», was dem Prinzip der praktischen Konkordanz gleichkommt.[18] Im Folgenden sollen die anfangs erwähnten Erlaubnistatbestandsmerkmale für die Verarbeitung von personenbezogenen Daten für Zwecke des Beschäftigungsverhältnisses näher beschrieben werden.

1) Erforderlichkeit für das Beschäftigungsverhältnis (§ 26 I S. 1 BDSG n. F.) – diese ist nicht mit dem zuvor erläuterten grundlegenden Verhältnismäßigkeitsgrundsatz zu verwechseln. Das Bundesarbeitsgericht (BAG) lässt nach bisheriger Rechtsprechung auch eine zukünftige Erforderlichkeit der Daten genügen.[19]

2) Aufdeckung von Straftaten (§ 26 I S.2 BDSG n. F) – Besonderheit ist hier, dass eine restriktive Auslegung anzunehmen ist. Literatur und Rechtsprechung sind der Auffassung, dass tatsächliche Anhaltspunkte für eine Straftat vorliegen müssen, bloße Gerüchte sind beispielsweise nicht ausreichend.[20]

3) Kollektivvereinbarung (§ 26 I S.1, IV BDSG n. F.) – Voraussetzung ist, dass sowohl die Anforderungen des Art. 88 II DSGVO als auch die Normen der Betriebsvereinbarung nach dem Betriebsverfassungsgesetz erfüllt sind. Aufgrund der Gültigkeit für alle Arbeitnehmer eines Betriebs kommt der Betriebsvereinbarung große praktische Relevanz zu.

4) Einwilligung (§ 26 II BDSG) – die hier genannte Einwilligung steht der «normalen» Datenverarbeitung gem. Art. 6 DSGVO gleich. Jedoch verlangt § 26 II BDSG n. F. zur Beurteilung der Freiwilligkeit einer solchen Einwilligung im Beschäftigungsverhältnis eine Berücksichtigung der Abhängigkeit und die Umstände, unter denen die Einwilligung erteilt wurde (vgl. § 26 II S. 2 BDSG n. F.). Die Gesetzesbegründung nennt als zulässige Beispiele etwa die betriebliche Gesundheitsförderung oder die private Nutzung von IT-Systemen. Ein höheres Entgelt kann jedoch nicht von einer Einwilligung abhängig gemacht werden. Dies verstieße gegen das in Art. 7 IV DSGVO normierte Kopplungsverbot.[21]

Aufgrund der geringen Regelungstiefe des Arbeitnehmerdatenschutzes bietet es sich an, Vorgaben und Empfehlungen aus den allgemeinen Anforderungen der DSGVO sowie der bestehenden Rechtsprechung abzuleiten. Das Hauptaugenmerk der allgemeinen Anforderungen der DSGVO dürfte bei der Umsetzung der Grundsätze (Art. 5–11 DSGVO) sowie der Betroffenenrechte (Art. 12–22 DSGVO) liegen. Es besteht eine umfangreiche Rechtsprechung im Bereich der Videoüberwachung. In dieser werden die Eingriffsintensität und die Betroffenenrechte den Arbeitgeberinteressen gegenübergestellt. Es wird zwischen einer eingriffsintensiven Form (heimliche Überwachung) und einer weniger eingriffsintensiven Form (offene Überwachung) unterschieden. Diese Systematik kann auch für neue technische Entwicklungen wichtige Leitlinien bereitstellen, etwa bei der Ortung von Arbeitnehmern für das Flottenmanagement oder bei der Nutzung von Biometrie anstelle von Passwörtern.

---

15 Maschmann, a.a.O., § 26 BDSG, Rn. 5.

16 Zöll, Oliver, § 26 BDSG Rn. 39. In: DSGVO – BDSG, Taeger, Jürgen/Gabel, Detlev (Hrsg.), dfv, 3. Auflage, 2019.

17 Vgl. Daten für die Begründung, Durchführung, Beendigung eines Beschäftigungsverhältnisses; Stammdaten (s.o.).

18 BT-Drs. 18/11325, S. 96; Maschmann, a.a.O., § 26 BDSG, Rn. 18; Franzen, Martin, § 26 BDSG Rn. 10f. In Erfurter Kommentar zum Arbeitsrecht, Dieterich, Thomas/Hanau, Peter/Schaub, Günter (Hrsg.), C.H. Beck, 19. Auflage, 2018; BAG, 20.06.2013 – 2 AZR 546/12.

19 Franzen, a.a.O., § 26 BDSG Rn. 9; BAG, 22.10.1986 – 5 AZR 660/85.

20 Maschmann, a.a.O., § 26 BDSG, Rn. 56–58; BAG, 20.10.2016 – 2 AZR 395/15; BAG 27.07.2017 – 2 AZR 681/16.

21 Franzen, a.a.O., § 26 BDSG Rn. 40–42.

In der praktischen Anwendung zeigt sich ein Bedürfnis nach (technischen) Lösungen, welche Transparenz für den einzelnen Mitarbeiter schaffen und diesem Kontrolle über die Verarbeitungsvorgänge geben, etwa indem er diesen widersprechen kann.

3. Technische Lösungskonzepte zur Einführung von Datenschutztechnologien in Organisationen

Datenschutztechnologien können Organisationen als Grundlage für die Umsetzung eines technologiegestützten Beschäftigtendatenschutzes dienen. Aktuell wird speziell der Einsatz von Privacy Dashboards[22] (PDBs) und den damit einhergehenden Datenschutztechnologien geprüft[23], die es Arbeitgebern ermöglichen ihren datenschutzrechtlichen Anforderungen nachzukommen und Arbeitnehmern Transparenz und Kontrolle bieten. PDBs haben sich bereits in anderen Kontexten für die Herstellung von Transparenz und Selbstbestimmung bei der Verwendung personenbezogener Daten bewährt[24] und sind als hilfreich bei der Umsetzung gesetzlicher Rahmenbedingungen identifiziert worden[25]. Insbesondere in Organisationen bedarf es verschiedener harmonisierter Konzepte, die die besonderen Umstände des Arbeitgeber-Arbeitnehmer-Verhältnisses bei der Einführung neuer Technologien berücksichtigen (vgl. Kapitel 4). Um diesen Herausforderungen zu begegnen und die Implementation eines Beschäftigtendatenschutzes zu ermöglichen, schlagen wir ein mehrstufiges Einführungskonzept (Stufenkonzept) vor, wie es im Folgenden näher erläutert wird.

Das von uns entwickelte Stufenkonzept (vgl. Abbildung 1) sieht fünf mögliche Ausbaustufen eines technologiegestützten Beschäftigtendatenschutzes vor. Es ermöglicht eine schrittweise Entwicklung und Einführung von PDBs sowie den dazugehörigen Datenschutztechnologien in Unternehmen und Organisationen. Höhere Stufen gehen mit einer zunehmenden technischen Integration einher, wodurch zunehmend mehr Kontrollmöglichkeiten von Datenflüssen bereitgestellt werden, gleichzeitig jedoch auch die Komplexität der Implementation zunimmt.

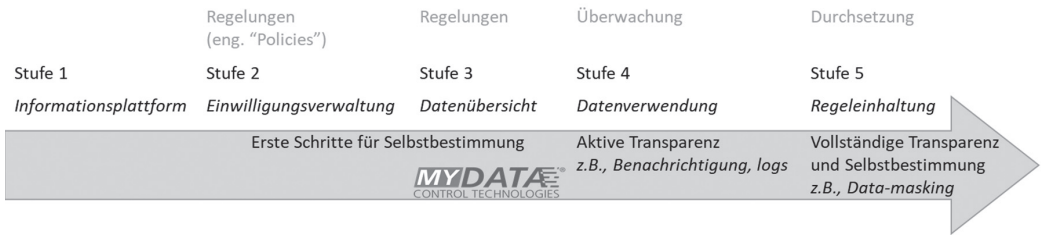

Abbildung 1 Gesamtübersicht des Stufenkonzepts

[22] Vgl. Polst, Svenja/Kelbert, Patricia/Feth, Denis, Company Privacy Dashboards: Employee Needs and Requirements, HCI for Cybersecurity, Privacy and Trust, 2019, S. 429–440.

[23] Bspw. wird im BMBF geförderten Projekt «TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen» ein praxistauglicher, rechtskonformer und technologiegestützter Beschäftigtendatenschutz realisiert. (https://www.trusd-projekt.de).

[24] Vgl. Zimmermann, Christian/Accorsi, Rafael/Müller, Günter, Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy, Ninth International Conference on Availability, Reliability and Security, 2014, S. 152–157; Angulo, Julio/Fischer-Hübner, Simone/Pulls, Tobias/Wästlund, Erik, Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures. In: Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems – CHI EA '15, Seoul, 2015, S. 1803–1808.

[25] Vgl. Heinemann, Andreas/Straub, Tobias, Datenschutz muss benutzbar sein: Wie Usable Security and Privacy die Ausübung von Betroffenenrechten erleichtern kann, DuD, Bd. 43, Nr. 1, S. 7–12, Jan. 2019; Raschke, Philip/Küpper, Axel/Drozd, Olha/Kirrane, Sabrina, Designing a GDPR-Compliant and Usable Privacy Dashboard. In: Privacy and Identity Management. The Smart Revolution, Hansen, Marit/Kosta, Elenia/Nai-Fovino, Netherlandslgor/Fischer-Hübner, Simone (Hrsg.), Springer International Publishing, 2018, S. 221–236.

Stufe 1 sieht die Bereitstellung einer Informationsplattform vor, in der sich Mitarbeiter über rechtliche Regelungen und unternehmensspezifische Datenverarbeitungen informieren können. Der Inhalt der Informationsplattform muss durch einen verantwortlichen Mitarbeiter der Organisation eingepflegt werden. Es gibt keine technische Integration in die Organisationsinfrastruktur oder Alt- bzw. Bestandssysteme.

Stufe 2 ermöglicht es einer Person, über ein PDB die Einwilligung zur Verarbeitung von Daten einer anderen Person anzufragen. Diese Person hat die Möglichkeit, diese Anfrage zu beantworten und Einstellungen zu hinterlegen. Es existiert jedoch keine technische Kontrolle darüber, ob und wie konkrete Daten tatsächlich verwendet werden und ob eine Einwilligung dafür vorliegt.

Stufe 3 setzt eine technische Teilintegration eines PDBs in bestehende Systeme voraus und gestattet eine dynamische Erfassung und aufbereitete Darstellung von Mitarbeiterdaten. Beschäftigte können über ein PDB einsehen, wer berechtigt ist, bestimmte Daten zu verarbeiten.

Stufe 4 erfordert eine vollumfängliche technische Integration eines PDBs und dazugehöriger transparenzfördernder Technologien (engl. Transparency Enhancing Technologies) in bestehende IT-Systeme. Dadurch erhalten Beschäftigte die Möglichkeit, die Verarbeitung ihrer personenbezogenen Daten zu überwachen, sodass bspw. auch unrechtmäßige Zugriffe erfasst und protokolliert werden können.

Stufe 5 ermöglicht die Durchsetzung von Berechtigungen und Regelwerken, die von Arbeitnehmer und Arbeitgeber (einvernehmlich) spezifiziert wurden. Durch den Einsatz privatheitsfördernder Technologien lässt diese letzte Ausbaustufe die Durchsetzung von diversen Datenschutzzielen zu. Diese Stufe ist gekennzeichnet durch ein vollumfängliches zentrales Datenmanagement und eine vollumfängliche technische Integration in die Zielanwendung. Berechtigungen werden nun technisch durchgesetzt.

Insbesondere durch die Anforderungen aus Stufe 4 und Stufe 5 ergibt sich die Notwendigkeit einer vollumfänglichen technischen Integration geeigneter Technologien in eine IT-Infrastruktur. Die vom Fraunhofer IESE entwickelten MYDATA Control Technologies (kurz MYDATA)[26] stellen die dazu benötigte technische Datennutzungskontrolle bereit, indem sie in sicherheits- und privatheitsrelevante Datenflüsse und -verarbeitungen eingreifen können. Benachrichtigungs- und Einwilligungsregeln werden als Policies erstellt und im Policy Management Point (PMP) verwaltet. Um die tatsächliche Datennutzung zu überwachen werden sogenannte Kontrollpunkte (engl. Policy Enforcement Points, PEPs) in diverse Zielsysteme integriert. In Stufe 4 beobachten PEPs lediglich Datenzugriffe. In Stufe 5 greifen PEPs aktiv in die Datenverarbeitung ein. Alle Ereignisse, die potenziell weiterer Entscheidungen oder Aktionen bedürfen, melden PEPs an eine weitere Komponente namens Policy Decision Point (PDP). Dort werden die in PMPs hinterlegten Regeln ausgewertet. Anschließend können sog. Policy Execution Points (PXPs) dazu angewiesen werden, bestimmte Aktionen durchzuführen, etwa Benachrichtigungen zu versenden oder Anonymisierungsverfahren anzuwenden.

4. Sozio-technische Gestaltung als Erfolgsfaktor

Neue Technologien und digitale Lösungen, wie die vorgestellten PDBs, können die Prozesse in Unternehmen und Organisationen an vielen Stellen unterstützen und Abläufe optimieren. Gleichzeitig bergen sie jedoch auch diverse Risiken in sich. Digitalisierung im Unternehmen bedeutet nicht nur die Einführung einer neuen Technologie, digitalen Lösung oder Software, sondern ist ein tiefgreifender Veränderungsprozess. Diese Erkenntnis geht auf den sozio-technische Systemansatz nach Ulich zurück, wonach die Einführung einer digitalen Lösung auf der technischen Seite auch die Organisation mit ihren Strukturen und Vereinbarungen sowie das soziale Gefüge im Unternehmen rund um den Menschen als Mitarbeiter beeinflussen kann.[27] Die erfolg-

[26] Feth, Denis/Jung Christian, 10 Jahre Forschung zu Datennutzungskontrolle am Fraunhofer IESE, 14.8.2019, https://blog.iese.fraunhofer.de/10-jahre-datennutzungskontrolle-am-fraunhofer-iese/, aufgerufen am 30. Oktober 2019.

[27] Vgl. Ulich, Eberhard, Arbeitspsychologie, 7. Auflage, Schäffel-Poeschel Verlag, 2011; Thul, Martin J., Der sozio-technische Systemansatz. In: Veränderungsprozesse erfolgreich gestalten, Zink, Klaus J./Kötter, Wolfgang/Longmuß, Jörg/Thul, Martin J. (Hrsg.), 2. Auflage, Springer Vieweg, 2015, S. 278–283.

reiche Einführung digitaler Lösungen ist daher als eine komplexe Gestaltungsaufgabe zu verstehen, die mehr als nur die technische Ebene im Unternehmen tangiert. Es müssen stets alle komplexen Zusammenhänge zwischen der technischen, organisationalen und mitarbeiterbezogenen Ebene beachtet werden, um den nachhaltig effektiven Einsatz und das Ausschöpfen des vollen Potenzials zu ermöglichen.[28] Wird dieses komplexe Zusammenwirken nicht hinreichend beachtet, kann es zu Schwierigkeiten bei der Umsetzung kommen: die ausgewählte Technologie entspricht ggf. nicht den Anforderungen am Arbeitsplatz, Mitarbeiter wurden nicht rechtzeitig geschult und sind überfordert oder der Betriebsrat bzw. die Personalvertretung sieht die Mitarbeiter unzulässig überwacht und blockiert den Einsatz. In der Praxis sind viele Szenarien denkbar, in denen ein effizienter Einsatz und das Ausschöpfen des vollen Potenzials einer digitalen Lösung nicht gelingen (können).

Mit dem Einsatz von PDBs wird Beschäftigten einerseits die Möglichkeit der Transparenz und Selbstbestimmung bzgl. der erhobenen personenbezogenen Daten gegeben. Andererseits werden sie im Kontext der Einführung und Nutzung eines PDB zumeist erst mit diesem Thema konfrontiert und setzen sich aktiv mit der Erhebung und Verwendung ihrer personenbezogenen Daten am Arbeitsplatz auseinander. Ohne eine vorherige Partizipation der Beschäftigten (soziale Ebene) und eine Anpassung der Prozesse (organisationale Ebene) kann die von den Mitarbeitern möglicherweise empfundene Überwachung vielfältige, nicht intendierte Auswirkungen entfalten. Denkbar ist beispielsweise, dass sich die Beschäftigten ständiger Kontrolle ausgesetzt fühlen und ihr Handeln bzw. Verhalten in einer Art und Weise anpassen, welche für sie selbst und/oder die organisationalen Prozesse und Arbeitsabläufe nachteilig ist.[29] Weitere Folgen können sein, dass das Vertrauensverhältnis zwischen Arbeitgeber und Arbeitnehmer gestört ist, Mitarbeiter versuchen die technische Lösung zu umgehen oder gezielt verfälschte Daten produzieren.[30] In der Praxis lassen sich viele Beispiele anführen, in denen Beschäftigte dies beim Einsatz technischer Lösungen versuchen, z. B. indem sie

– bei einer digitalen Zeiterfassung nach dem Ausstechen an den Arbeitsplatz zurückkehren und weiterarbeiten, um hierdurch betriebliche und/oder gesetzliche 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.

Darüber hinaus deutet einiges darauf hin, dass die Überwachung am Arbeitsplatz insgesamt zu einem Verlust der wahrgenommenen Kontrolle und zu einem gesteigerten subjektiven Stresserleben führt.[31]

Vor diesem Hintergrund ist bei der Entwicklung und Einführung von transparenzsteigernder Technologie zu berücksichtigen, dass ein solches Tool von den Beschäftigten als ein weiteres Managementwerkzeug mit dem Ziel einer umfassenderen Überwachung und besseren Steuerung der Mitarbeiter angesehen werden kann. Die Aspekte Überwachung, Kontrolle und Steuerung der Beschäftigten stehen damit zumindest implizit im Raum und sollten frühzeitig offen thematisiert werden. Ferner lassen die Ergebnisse bisheriger Untersuchungen in diesem Themenfeld darauf schließen, dass die intendierten und nicht-intendierten Auswirkungen der

---

[28] Vgl. Bosse, Christian/Hellge, Viola/Schröder, Delia/Dupont, Stephanie, Digitalisierung im Mittelstand erfolgreich gestalten. In: Arbeit 4.0 im Mittelstand. Chancen und Herausforderungen des digitalen Wandels für KMU, Bosse, Christian K./Zink, Klaus J. (Hrsg.), Springer Gabler 2019, S. 13–34.

[29] Vgl. dazu u.a. Rosenblat, Alex/Stark, Luke, Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers. International Journal of Communication, 10, 2016, S. 3758–3784; Da Cunha, Joao Vieira/Carugati, Andea/Leclercq-Vandelannoitte, Aurelie, The dark side of computer-mediated control. Information Systems Journal, 25, 2015, S. 319–354 sowie Pritchard, Gary W./Briggs, Pamela/Vines, John/Oliver, Patrick, How to Drive a London Bus: Measuring Performance in a Mobile and Remote Workplace. CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015 S. 907–916.

[30] Vgl. dazu u.a. Mohammad, Mohammad, IT Surveillance and Social Implications in the Workplace. Proceedings of the 2015 SIGMIS Conference on Computers and People Research, 2015, S. 79–85 und Pritchard et al. (2015) a.a.O.

[31] Vgl. Backhaus, Nils, Kontextsensitive Assistenzsysteme und Überwachung am Arbeitsplatz. Ein meta-analytisches Review zur Auswirkung elektronischer Überwachung auf Beschäftigte Zeitschrift für Arbeitswissenschaft, 73(1), 2019, S. 2–22.

Einführung einer neuen Technologie auf die Beschäftigten, welche zumindest theoretisch auch zu einer umfassenderen Überwachung und Kontrolle der Mitarbeiter eingesetzt werden könnte, ex ante nicht abschätzbar sind, sondern organisations- und personengruppenspezifisch variieren. In diesem Zusammenhang sind organisationsspezifische Besonderheiten ebenso zu berücksichtigen wie die individuellen Interessen und Anforderungen der Mitarbeiter. Es empfiehlt sich, bereits von Beginn an die (betroffenen) Mitarbeiter in den Veränderungsprozess einzubeziehen und ihre Kompetenzen und Qualifikationen ebenso wie bspw. bestehende Strukturen, Hierarchien, Arbeitsumgebung und Unternehmenskultur im Rahmen einer partizipativen Anforderungserhebung zu erfassen.[32] Bei der folgenden Entwicklung sind zum einen Aspekte wie Transparenz, Nachvollziehbarkeit und Vorhersagbarkeit für die Nutzer zu berücksichtigen, zum anderen müssen den Nutzern bei der Einführung adäquate Informationen über die Technologie sowie die Intention der Erhebung und Nutzung der personenbezogenen Daten zur Verfügung gestellt werden. Folglich ist die organisationsspezifische Ausgestaltung des Einführungsprozesses mit einer aktiven Einbindung der Mitarbeiter zur Anforderungserhebung, Sensibilisierung und Qualifizierung einer der zentralen Erfolgsfaktoren des nachhaltigen Einsatzes transparenzsteigernder Technologie.

5. Fazit

Privacy Dashboards bzw. deren stufenweise Einführung, wie sie in diesem Beitrag vorgeschlagen wird, ermöglichen Unternehmen eine rechtskonforme Umsetzung des Beschäftigtendatenschutzes. Sie schaffen Transparenz über die im Arbeitskontext erhobenen personenbezogenen Daten und stärken auch im Sinne der Arbeitnehmer und deren Vertreter aktiv die Möglichkeiten der Selbst- und Mitbestimmung. Um diese Potenziale auszuschöpfen, ist es erforderlich, die Veränderungen in einem strukturierten Change-Management-Prozess aktiv zu gestalten.[33] Sogenannte Change-Management-Prozesse sind vielen Unternehmen nicht unbekannt, werden sie doch seit Jahren bereits in verschiedenen Ausgangssituationen eingesetzt, bspw. bei der Neuausrichtung eines bestehenden Unternehmens oder bei organisationalen Zusammenschlüssen mehrerer Unternehmenseinheiten. Die Herausforderungen im Kontext einer Einführung neuer Technologien wie bspw. eines PDBs und das Voranschreiten der digitalen Transformation von Unternehmen allgemein werden zukünftig vermehrt der Auslöser für Veränderungsprozesse sein.[34] Hierbei bietet es viele Vorteile, den Veränderungsprozess formal, proaktiv und strategisch zu gestalten, anstatt reaktiv auf auftretende Probleme, Verunsicherung und Ablehnung zu reagieren.[35]

6. Danksagung

Diese Arbeit wurde durch das Forschungsprojekt «TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen» unterstützt, finanziert durch das deutsche Bundesministerium für Bildung und Forschung (BMBF).

[32] Vgl. hierzu u.a. Kötter/Zink, a.a.O., S. 283–286.

[33] Vgl. Schlicher, Katharina. D./Paruzel, Agnieszka/Steinmann, Barbara/Maier, Günter W., Change Management für die Einführung digitaler Arbeitswelten. In: Handbuch Gestaltung digitaler und vernetzter Arbeitswelten, Maier, Günter W./Engels, Gregor/Steffen, Eckhard (Hrsg.), Berlin, Heidelberg: Springer, 2018.

[34] Vgl. Schlicher et al. a.a.O.

[35] Vgl. Cawsey, Tupper F./Deszca, Gene/Ingols, Cynthia A., Organizational change, 3. Auflage, Los Angeles Sage, 2016.