EINWILLIGUNG ODER ANONYMISIERUNG? RECHTLICHE IMPLIKATIONEN DER DATENVERARBEITUNG IM BESCHÄFTIGUNGSKONTEXT

Bianca Steffes / Christian K. Bosse / Aljoscha Dietrich / Hartmut Schmitt

Wissenschaftliche Mitarbeiterin, Lehrstuhl für Rechtsinformatik, Universität des Saarlandes, 66123 Saarbrücken, DE, bianca.steffes@uni-saarland.de, https://www.legalinf.de

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

Datentreuhänder, Landkreis Sankt Wendel, Mommstr. 29, 66606 St. Wendel, DE, a.dietrich@lkwnd.de, https://digitalregion.landkreis-st-wendel.de

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

Schlagworte: ***DSGVO, BDSG, Beschäftigungsverhältnis, Einwilligung, Anonymisierung***

Abstract: *Datenverarbeitungen im Beschäftigungsverhältnis unterliegen dem Schutz der DSGVO und des BDSG. Durch diese Normen werden verschiedene Wege für eine rechtskonforme Datennutzung ermöglicht, die wir mit ihren Anwendungsmöglichkeiten und Einschränkungen erläutern. Neben möglichen Rechtsgrundlagen wie der Einwilligung thematisieren wir die Anonymisierung von Daten, mit der die Anwendbarkeit des Datenschutzrechts vermieden werden kann. Abschließend geben wir eine Entscheidungshilfe zur Anwendung der Vorgehensweisen im Beschäftigungsverhältnis.*

1. Motivation

Die Digitalisierung der Arbeitswelt und der zunehmende Einsatz neuer Technologien wie künstlicher Intelligenz eröffnen Unternehmen die Möglichkeit, in bislang nicht gekanntem Ausmaß Daten zu verarbeiten. Auf Basis der Datenanalyse können Entscheidungsträger Vorteile für ihre Unternehmen erzielen, beispielsweise durch die Gestaltung effizienterer und kostensparender Arbeitsprozesse. Findet eine Verarbeitung personenbezogener Daten von Beschäftigten[1] statt, so kann dies jedoch die informationelle Selbstbestimmung der Beschäftigten gefährden und einen unzulässigen Eingriff in deren Privatsphäre bedeuten, etwa wenn die Grenze zur unzulässigen Überwachung überschritten wird.[2]

Die sich gegenüberstehenden Interessen von Arbeitgebern und Arbeitnehmern beschreibt Thüsing[3] als *Grundkonflikt* im Arbeitnehmerdatenschutz: Der Arbeitgeber will sicherstellen, dass die Beschäftigten ihre arbeitsvertraglichen Pflichten erfüllen, Dateneinrichtungen nicht missbrauchen und Betriebseigentum nicht beschädigen. Dem steht der Wunsch der Beschäftigten gegenüber, vor fortlaufender Überwachung und Kontrolle geschützt zu werden und in dem Wunsch nach Privatheit und informationeller Selbstbestimmung respektiert zu werden. Ein Beispiel verdeutlicht dies: Bewegungsdaten der Beschäftigten, die in einem Warenlager

[1] Im Folgenden werden die Begriffe ‚Arbeitnehmer' und ‚Beschäftigte' synonym verwendet.

[2] Vgl. Bosse/Dietrich/Kelbert/Küchler/Schmitt/Tolsdorf/Wessner, Beschäftigtendatenschutz: Rechtliche Anforderungen und Technische Lösungskonzepte, IRIS 2020.

[3] Vgl. Thüsing, Arbeitnehmerdatenschutz und Compliance. C.H.Beck, 2010, S. 1.

gewonnen werden, können einerseits genutzt werden, um ineffiziente Abläufe aufzudecken und das Lager besser zu organisieren. Andererseits kann der Arbeitgeber auf Basis ständig erhobener Daten unzulässige Bewegungsprofile erstellen, einschließlich des Verhaltens der Beschäftigten in den Arbeitspausen und über die Grenzen des Betriebsgeländes hinaus. Daneben gibt es aber auch Fälle, in denen Arbeitgeber und Arbeitnehmer *gleichgelagerte Interessen* haben: Werden beispielsweise anhand von Sensordaten, die in einer intelligenten Fabrik gesammelt werden, falsche Bewegungsmuster der Beschäftigten aufgedeckt, so kommt die dadurch ermöglichte Vermeidung von Gesundheitsproblemen sowohl dem Arbeitgeber als auch den Arbeitnehmern zugute.

In Deutschland existiert bislang kein Beschäftigtendatenschutzgesetz, allerdings wird dies seit mehreren Jahrzehnten auf politischer und rechtswissenschaftlicher Ebene diskutiert. Aktuell erörtert ein „Beirat zum Beschäftigtendatenschutz“[4] Bedarf und Spielraum. Grundsätzlich findet die Datenschutzgrundverordnung (DSGVO) Anwendung, deren Regelungen aber erkennbar nicht auf den Beschäftigtendatenschutz zugeschnitten sind[5] und die in Art. 88 Abs. 1 eine Öffnungsklausel für den Beschäftigtendatenschutz enthält. Die maßgebliche – aber nicht ausschließliche – Norm in Deutschland ist § 26 Bundesdatenschutzgesetz (BDSG), „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“.[6]

Ziel dieses Beitrags ist es, aufzuzeigen, welche Möglichkeiten der rechtskonformen Datennutzung es gibt, und gleichzeitig eine Entscheidungshilfe zu geben, wann welches Vorgehen sinnvoll ist. Dem Beschäftigtendatenschutz kommt hierbei nicht nur die Funktion zu, die Beschäftigten zu schützen, sondern gleichzeitig deren Vertrauen in neue Technologien wie Big Data und künstliche Intelligenz zu stärken.[7] Neben Fragen der Rechtskonformität thematisieren wir auch Auswirkungen, die die Verarbeitung personenbezogener Daten auf anderen Ebenen haben kann, beispielweise wenn permanentes Überwachungsgefühl und Leistungsdruck für ein höheres Stresslevel und einen Verlust der intrinsischen Motivation sorgen und dadurch auch für den Arbeitgeber Nachteile implizieren.[8]

2. Datenklassen

Die personenbezogenen Daten der Beschäftigten, die beim Einsatz digitaler Technologien im Arbeitsumfeld anfallen, können aus unterschiedlichen Bereichen stammen – z. B. Personalbereich, digitale Zusammenarbeit oder (zulässige) Leistungsüberwachung – und entsprechend unterschiedlich aufgebaut sein. Im Projekt TrUSD[9] wurde als Teil eines Rahmenwerks für den technologiegestützten Beschäftigtendatenschutz eine *Ontologie* entwickelt, die einen Überblick über typische *Datenklassen* im Bereich Beschäftigtendatenschutz ermöglicht. Die konkrete Ausgestaltung und das zugrundeliegende Datenmodell können branchen- und unternehmensspezifisch angepasst werden. Daher gibt das Rahmenwerk eher generische Datenklassen mitsamt typischen Beispielen für Unterklassen vor, die allerdings nicht als abschließende Klassenhierarchie zu verstehen sind (siehe Tabelle 1).

---

4 Vgl. Bundesministerium für Arbeit und Soziales, Faktenblatt „Beirat zum Beschäftigtendatenschutz“, https://www.bmas.de/SharedDocs/Downloads/DE/Pressemitteilungen/2020/faktenblatt-beirat-zum-beschaeftigtendatenschutz.pdf, (aufgerufen am 05.11.2021), 2020.

5 Vgl. Wybitul, Kommt bald ein neues Gesetz zum Beschäftigtendatenschutz?, https://www.cr-online.de/blog/2020/06/20/neues-gesetz-zum-beschaeftigtendatenschutz/ (aufgerufen am 05.11.2021), 2020.

6 Vgl. Wybitul, a.a.O.

7 Vgl. Bundesministerium für Arbeit und Soziales, Beschäftigtendatenschutz, https://www.bmas.de/DE/Arbeit/Digitalisierung-der-Arbeitswelt/Denkfabrik-Digitale-Arbeitsgesellschaft/beschaeftigtendatenschutz.html (aufgerufen am 05.11.2021), 2020.

8 Vgl. Morlok/Matt/Hess, White Paper: „Privatheit und Datenflut in der neuen Arbeitswelt: Chancen und Risiken einer erhöhten Transparenz“, Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, 2015, S. 5.

9 Weitere Informationen zum Projekt TrUSD können unter https://www.trusd-projekt.de/ gefunden werden.

Datenklassen	Unterklassen (Beispiele)
Daten zur Person	Stammdaten, besondere Kategorien personenbezogener Daten, Zertifikate und Bescheinigungen, Bilder und Videos
Daten zum Beschäftigungsverhältnis	administrative Daten, Daten zur Dokumentation der Arbeit
Arbeitsinhalte und -ergebnisse	berufliche Termine, Kooperationspartner und Auftraggeber, Aktivitäten
Kommunikationsdaten	Kontakte, Kommunikationsverhalten, Kommunikationsinhalte
Standortdaten	Reisen und Reisezeiten, Mobilitätsdaten
technische Daten	Geräte, Berechtigungen, Protokolldaten, Datenschutzeinstellungen
private Daten	private Kontaktdaten, private Termine, Freizeit- und Konsumverhalten, Informationen über persönliche Probleme

Tabelle 1: Datenklassen und Beispiele typischer Unterklassen

Einen besonderen Schutz – auch jenseits des Beschäftigungskontexts – genießen nach Art. 9 DSGVO besondere Kategorien personenbezogener Daten. Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische Daten, biometrische Daten, Gesundheitsdaten und Daten zum Sexualleben und zur sexuellen Orientierung.

Hinsichtlich der Maßnahmen, die im Folgenden vorgestellt bzw. diskutiert werden, ist zu beachten, dass nicht alle beschriebenen Maßnahmen auf sämtliche Datenklassen anwendbar sind. Vielmehr wird man oft abhängig vom Anwendungsfall oder Verarbeitungszweck entscheiden müssen, ob bestimmte Daten anonymisiert oder verrauscht werden können bzw. ob und von welchem Anwender sie dann noch sinnvoll genutzt werden können. Ein Beispiel:[10] Ein Wartungsunternehmen hat seine Firmenfahrzeuge mit GPS-Ortungssystemen ausgestattet. Durch eine Gerätezuordnung zu den jeweiligen Beschäftigten ist ein Personenbezug möglich. Damit dringende Störungen durch möglichst nahe Fahrzeuge zügig beseitigt werden können, greift die zuständige Stelle im Bedarfsfall auf die GPS-Ortung zu. In diesem Anwendungsfall muss keine dauerhafte Erhebung der Positionsdaten erfolgen, sondern nur dann, wenn die Notwendigkeit besteht, einen dringenden Auftrag kurzfristig zu bearbeiten. Im selben Unternehmen gibt es außerdem Sonderfahrzeuge, deren genaue Einsatzzeiten für Abrechnungszwecke zweifelsfrei belegt werden müssen. Bei diesem Anwendungsfall werden die Positionsdaten der Fahrzeuge daher konstant erhoben und zeitweilig gespeichert.

3. Anonymisierung

Aus rechtlicher Sicht ist der Einsatz von *Anonymisierung* eine Möglichkeit, die Anwendbarkeit der DSGVO zu vermeiden. Die Anonymisierung wird in der DSGVO indirekt in Erwägungsgrund 26 S. 5 und 6 genannt. Die DSGVO gilt demnach nicht, wenn „die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Jedoch legt der gleiche Erwägungsgrund in S. 3 und 4 fest, dass es sich nicht unbedingt um eine feste Eigenschaft handelt, ob ein Datum als personenbezogen bzw. als anonym einzustufen ist. Es sollen nämlich „alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren [...]“. Hierfür gilt, dass „[...] die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.“ Dies bedeutet, dass der Gesetzgeber explizit berücksichtigt, dass die

[10] Vgl. Die Landesbeauftragte für den Datenschutz Niedersachsen, Typische Fälle im Beschäftigtendatenschutz, https://lfd.niedersachsen.de/download/127627/Typische_Fallbeispiele_im_Beschaeftigtendatenschutz_Stand_November_2018_.pdf (aufgerufen am 05.11.2021), 2018.

Feststellung der Anonymität auch der technologischen Entwicklung unterliegt. In diesem Kontext interessant ist der Aufrufe zu einem Verbot einer De-Anonymisierung, analog zu der Rechtslage in Japan.[11] Fraglich ist, welche Auswirkung ein Verbot auf die Forschung hätte, welche sich mit den technischen Möglichkeiten der De-Anonymisierung bzw. der Erforschung von Schwachstellen auseinandersetzt.[12]

Aus technischer Sicht gibt es ein breites Spektrum an Anonymisierungsmethoden, die auch in der Übersichtsarbeit von Winter et al.[13] dargestellt werden. Hier wollen wir die zwei bekanntesten Methoden der Anonymisierung darstellen. Da die Anonymisierung von Daten den kompletten Personenbezug entfernt, betrachten diese Methoden stets eine Menge an Daten (Datenbank), die von unterschiedlichen Personen stammen (ein Datensatz pro Person). Denn wäre nur ein einziger Datensatz vorhanden, so ist oftmals leicht daraus zu folgern, zu welcher Person er gehört. Das reine Entfernen des direkten Identifikators, etwa des Namens, stellt dabei keine zuverlässige Anonymisierungsmethode dar, da beispielsweise Kombinationen von Geburtsdatum, Postleitzahl und Geschlecht ebenfalls in vielen Fällen eine Identifizierung ermöglichen.[14]

Generalisierung

Bei der Anonymisierung durch Generalisierung sollen identifizierende Informationen derart eingeschränkt oder generalisiert werden, dass die Zuordnung zu einer bestimmten Person verhindert wird. Samarati et al. benannten diese Teilemenge der Attribute der Datenbank, deren Veröffentlichung (zum Erhalt der Anonymität) eingeschränkt werden muss, als Quasi-Identifikator.[15] Diese Attribute sind zumeist (öffentlich) bekannt[16] und beinhalten nicht die sensiblen Informationen der Datenbank.

Ein bekanntes Konzept nach diesem Schema ist die *k-Anonymität*, die ursprünglich von Samarati und Sweeney definiert wurde.[17] Ihnen zufolge liegt k-Anonymität genau dann vor, wenn jede vorhandene Wertkombination des Quasi-Identifikators in der Datenbank insgesamt mindestens k-mal vorkommt. Um diesen Zustand zu erreichen, werden beispielsweise die Werte des Quasi-Identifikators so lange generalisiert, bis sich mindestens k Zeilen (in unserem Fall: Datensätze) im Quasi-Identifikator entsprechen.

Dadurch, dass die Anonymisierung in der Generalisierung des Quasi-Identifikators liegt und keine Änderungen an den sensiblen Informationen des Datensatzes vorgenommen werden, kann die Methode auf jede Datenklasse aus Abschnitt 2 angewendet werden. Das ursprüngliche Verfahren der k-Anonymität hat jedoch im Laufe der Zeit einige Schwächen offenbart, die mit Erweiterungen wie der *l-Diversität*[18] oder auch *t-Closeness*[19] behoben wurden. Dennoch ist die Diskussion über die Sicherheit von k-Anonymität noch nicht abgeschlossen, wie Cohen[20] zeigt. Hinzu kommt die Problematik des Bestimmens des Quasi-Identifikators: Vorhandene Ansätze wie die von Mansour et al.[21] oder Motwani et al.[22] basieren auf Annäherungen und

[11] Vgl. Rossnagel/Geminn: Vertrauen in Anonymisierung, ZD 2021, S. 488 ff.

[12] Vgl. Sorge, Empirische Forschung im technischen Datenschutz: Ein juristisches Problem?, Abstraktion und Applikation: IRIS 2013, S. 469–474.

[13] Vgl Winter/Battis/Halvani, Herausforderungen für die Anonymisierung von Daten, ZD 11/2019, 2019, S. 489–493.

[14] Vgl. Sweeney, Weaving technology and policy together to maintain confidentiality, J Law Med Ethics, 1997 Summer-Fall, 25(2–3), S. 98–110.

[15] Vgl. Samarati/Sweeney, Protecting Privacy when Disclosing Information: k-Anonymity and its Enforcement through Generalization and Suppression, In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, 1998.

[16] Vgl. Dalenius, Finding a needle in a haystack or identifying anonymous census records, J Off Stat 2(3), 1986, S. 329–336.

[17] Vgl. Samarati/Sweeney, a.a.O.

[18] Vgl. Machanavajjhala/Kifer/Gehrke/Venkitasubramaniam, l-Diversity: Privacy beyond k-anonymity, ACM Trans. Knowl. Discov. Data, 2007.

[19] Vgl. Li/Li/Venkatasubramanian, t-Closeness: Privacy Beyond k-Anonymity and l-Diversity, 2007 IEEE 23rd International Conference on Data Engineering, 2007, S. 106–115.

[20] Vgl. Cohen, The Quasi-identifiers are the Problem: Attacking and Reidentifying k-Anonymous Datasets, working paper, (zuletzt abgerufen: 11.10.2021), 2021.

[21] Vgl. Mansour/Siraj/Ghaleb/Saeed/Alkhammash/Maroof, Quasi-Identifier Recognition Algorithm for Privacy Preservation of Cloud Data Based on Risk Reidentification, Hindawi, Wireless Communications and Mobile Computing. Volume 2021.

[22] Vgl. Motwani/Xu, Efficient Algorithms for Masking and Finding Quasi-Identifiers, P3DM'08, 2008.

können den Quasi-Identifikator nicht immer exakt bestimmen. Wird ein unvollständiger Quasi-Identifikator in die Generalisierung aufgenommen, so besteht keine echte k-Anonymität und folglich auch keine Garantie für Anonymität.

Aggregation

Die Anonymisierung durch Aggregation basiert auf der Annahme, dass aggregierte Daten keinen Rückschluss mehr auf Personen zulassen. Aggregatfunktionen ermöglichen es dabei, Daten zusammenzufassen.[23] Beispielsweise könnten hier der Mittelwert oder das Maximum eines Attributs berechnet werden oder die Anzahl eines bestimmten Wertes (bspw. Personen des gleichen Namens) gezählt werden. Diese Funktionen bringen jedoch Einschränkungen bezüglich der Datentypen mit sich: Das Berechnen von algebraischen Aggregatfunktionen (bspw. Mittelwert) ist nur auf Zahlen möglich und eignet sich nicht für nominal- oder ordinalskalierte Daten wie Namen oder Telefonnummern. Diese Daten eignen sich ebenfalls nur bedingt für distributive Aggregatfunktionen, die Aussagen über die Verteilung eines Attributes treffen (bspw. die Anzahl einer bestimmten Ausprägung eines Attributes): Telefonnummern etwa sind meist einzigartig und tauchen dementsprechend in Datenbanken mit hoher Wahrscheinlichkeit nur einmal auf.

In der wissenschaftlichen Arbeit mit statistischen Tabellen, die ebenfalls Aggregationen nutzen, hat sich herausgestellt, dass es unmöglich ist, eine statistische Datenbank zu veröffentlichen, die keinen zusätzlichen Informationsgewinn über Individuen zulässt.[24] Daher ist eine reine Aggregation keine sichere Anonymisierungsmethode. Folglich hat man sich darauf konzentriert, zu verhindern, dass mögliche Angreifer durch das Vorhandensein eines Datensatzes in einer statistischen Tabelle erheblich mehr Informationen über die Person erhalten können, als wenn deren Datensatz nicht in der Tabelle vorkommt. Dadurch sollen Personen keinen signifikanten Nachteil erhalten, wenn sie ihre Daten für Berechnungen zur Verfügung stellen. Das aus dieser Forschung resultierende Konzept trägt den Namen *Differential Privacy* und wurde grundlegend von Dwork definiert.[25, 26] Eine konkrete Ausprägung ist dabei ε-*Differential Privacy*, wobei ε der Parameter zur Wahl der garantierten Privacy darstellt.[27]

Differential Privacy arbeitet mit der Annahme, dass jede Anfrage oder Berechnung auf einer Datenbank einen gewissen Grad an Informationen preisgibt. Wie hoch dieser Informationsgehalt ist, hängt dabei von der Berechnung ab (Sensitivity).[28] Um den offengelegten Informationsgehalt über Individuen niedrig zu halten und dennoch die Nutzbarkeit der Daten zu optimieren, liefern Anfragen auf Daten, die durch Differential Privacy geschützt sind, leicht ungenaue Ergebnisse zurück, wobei die Ungenauigkeit von der Sensitivity, der Anzahl der Elemente in der Datenbank und dem Parameter ε abhängt.[29] Da durch dieses Rauschen jedoch nicht komplett verhindert werden kann, dass Erkenntnisse über Individuen gewonnen werden, verwaltet Differential Privacy ein Privacy Budget (festgelegt durch ε), das mit jeder Berechnung entsprechend der Sensitivity verringert wird. Ist dieses Budget aufgebraucht, dürfen keine Informationen mehr aus diesem Datensatz preisgegeben werden und die Daten müssen somit verworfen werden,[30] wobei nicht jeder Anwendungsfall das komplette Privacy Budget benötigt. Problematisch an dem Ansatz ist jedoch oft, dass unklar ist, welcher Wert für ε angemessen ist. Tatsächlich gibt es keine allgemeingültige Empfehlung für ε, sondern es muss ein

---

23 Vgl. van Renesse, The Importance of Aggregation, Future Directions in Distributed Computing, Springer-Verlag, 2003, S. 87–92.

24 Vgl. Dwork, Differential privacy, Automata, languages and programming, Springer Berlin Heidelberg, 2006, S. 1–12.

25 Vgl. Dwork 2006, a.a.O.

26 Vgl. Dwork, Differential privacy: a survey of results, In Proceedings of the 5th international conference on Theory and applications of models of computation (TAMC'08). Springer-Verlag, Berlin, Heidelberg, 2008, S. 1–19.

27 Vgl. Dwork/Roth, The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, 2013.

28 Vgl. Dwork/McSherry/Nissim/Smith, Calibrating Noise to Sensitivity, in Private Data Analysis, Proceedings of the 3rd Theory of Cryptography Conference, 2006, S. 265–284.

29 Vgl. Dwork/Roth, a.a.O.

30 Vgl. Dwork/Roth, a.a.O.

individuelles Gleichgewicht zwischen Privacy und Nutzbarkeit gefunden werden, wie bspw. bei Hsu et al.[31] näher beleuchtet. Zusammengefasst lässt sich sagen, dass Differential Privacy zwar einen gewissen Grad an Anonymität bietet, jedoch nur auf bestimmten Datentypen arbeiten kann, leicht ungenaue Ergebnisse liefert und aufgrund des Privacy Budgets nur eine begrenzte Nutzung der Daten ermöglicht.

4. Erlaubnistatbestände

Die Verarbeitung personenbezogener Daten ist grundsätzlich nur dann zulässig, wenn ein Erlaubnistatbestand nach Art. 6 Abs. 1 DSGVO bzw. bei personenbezogenen Daten besonderer Kategorien zusätzlich eine Ausnahme nach Art. 9 Abs. 2 DSGVO vorliegt. Im Fall von Beschäftigtendaten hat der europäische Gesetzgeber jedoch eine Öffnungsklausel mit Art. 88 DSGVO eröffnet, die nationalen Regelungen für die Datenverarbeitung im Beschäftigtenkontext erlaubt. Diese Öffnungsklausel wurde durch den deutschen Gesetzgeber mit § 26 BDSG ausgefüllt.

Damit § 26 BDSG zur Anwendung kommt, muss zum einen der persönliche Anwendungsbereich eröffnet sein. Dieser liegt vor, wenn Beschäftigte gemäß § 26 Abs. 8 BDSG betroffen sind. Zudem muss der sachliche Anwendungsbereich eröffnet sein, wofür zusätzlich zu den Erfordernissen der DSGVO (Verarbeitung personenbezogener Daten nach Art. 2 Abs. 1 DSGVO) die Verarbeitung zu Zwecken des Beschäftigungsverhältnisses zu geschehen hat. § 26 BDSG gibt verschiedene Erlaubnistatbestände vor, darunter eine Konkretisierung der Einwilligung.[32]

Zu beachten ist hierbei insbesondere, dass durch § 26 Abs. 2 BDSG die Einwilligung im Beschäftigtenkontext spezifiziert wird und daher deutlich strengere Anforderungen gelten als für die „allgemeine“ datenschutzrechtliche Einwilligung gemäß Art. 7 DSGVO. Besondere Würdigung findet bei dieser Einwilligung im Beschäftigtenkontext die Berücksichtigung des Machtgefälles sowie das Abhängigkeitsverhältnis zwischen Arbeitgeber und Arbeitnehmer, schließlich könnte der Arbeitnehmer bei einer Ablehnung diverse Konsequenzen auf persönlicher Ebene bis hin zum Verlust seines Arbeitsplatzes befürchten. Dies spiegelt sich darin wider, dass eine „echte“ Freiwilligkeit vorzuliegen hat. Eine solche Freiwilligkeit kann insbesondere dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Gesetzesbegründung für das BDSG[33] liefert konkrete Beispiele, wann eine Freiwilligkeit gegeben sein kann: Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung, Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen, Aufnahme des Namens und Geburtsdatums in eine Geburtstagsliste und Nutzung von Fotos für das Intranet.

Eine vorherige Einstufung der zu verarbeitenden Daten in Datenklassen (vgl. Abschnitt 2) kann sich bei der Wahl eines passenden Erlaubnistatbestands als äußerst hilfreich erweisen. Bei den Datenklassen „Daten zum Beschäftigungsverhältnis” sowie „Arbeitsinhalte und -ergebnisse” ist etwa grundsätzlich eine Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses anzunehmen. Daten der Klasse “private Daten” dürften entsprechend nicht verarbeitet werden. Bei der Klassifizierung der Daten wäre demnach darauf zu achten, dass dies möglichst auf Grundlage des § 26 BDSG erfolgt.

Es stellt sich auch die Frage des Verhältnisses zwischen BDSG und DSGVO. Für die DSGVO gilt Anwendungsvorrang gegenüber nationalem Recht, sie gilt gemäß Art. 288 Abs. 2 AEUV unmittelbar in jedem Mitgliedsstaat. Aufgrund der Öffnungsklausel des Art. 88 DSGVO kann der nationale Gesetzgeber jedoch spezi-

[31] Vgl. Hsu/Gaboardi/Haeberlen/Khanna/Narayan/Pierce/Roth, Differential Privacy: An Economic Method for Choosing Epsilon, 2014 IEEE 27th Computer Security Foundations Symposium, 2014, S. 398–410.

[32] Zu weiteren Ausführungen vgl. Ströbel/Wybitul, § 10, in Handbuch Europäisches und deutsches Datenschutzrecht, Specht/Mantz (Hrsg.), 1. Aufl., 2019, Rn. 25 ff; sowie von den Autoren des Beitrags in Bosse et al. a.a.O., S. 179 ff.

[33] BT-Drs. 18/11325 S. 97.

fischere Regelungen im Beschäftigtenkontext vorgeben, welche dann der DSGVO vorgehen.[34] Fraglich ist, ob die Regelungen der DSGVO und des BDSG auch nebeneinander gelten können, also ob im Beschäftigtenkontext auch die Rechtfertigungstatbestände des Art. 6 Abs. 1 DSGVO zusätzlich Anwendung finden können.[35] Diese Meinung der parallelen Anwendung wird in der Literatur durchaus vertreten, § 26 BDSG verdrängt jedoch in seinem Anwendungsbereich des Beschäftigtendatenschutzes die Regelung des Art. 6 Abs. 1 UAbs. 1 lit. B DSGVO (Datenverarbeitung für die Erfüllung eines Vertrags).[36]

Die Abwägung zwischen den Interessen des Arbeitgebers und des Arbeitnehmers ist grundsätzlich die Essenz der einzelnen Erlaubnistatbestände im Beschäftigtendatenschutz, dahinter stehen in der Regel die tangierten Grundrechte der beteiligten Parteien. Für die Auslegung des § 32 BDSG a.F. entwickelte sich ein umfangreiches Richterrecht.[37] Aufgrund der Ähnlichkeit des § 26 BDSG zum § 32 BDSG ist ein Fortbestand des Richterrechts (vorerst) anzunehmen[38] und damit auch dessen Nachteile der fehlenden Ordnung und eingeschränkten Übertragbarkeit.[39] Grundsätzlich ist das Ergebnis einer Interessensabwägung im Regelfall äußert komplex und vielfach nicht eindeutig. Zur Unterstützung der Einhaltung der Regeln für die Einwilligung wurden bereits diverse Werkzeuge entwickelt.[40]

5. Diskussion und Anwendung

Mit dem rasanten Fortschritt der digitalen Transformation der Arbeitswelt, die zu einer Flut an auswertbaren Daten im Beschäftigungskontext führt, gewinnt der Schutz vor allem der personenbezogenen und besonders sensiblen Daten[41] immer mehr an Relevanz. Mit Hilfe von Verordnungen und Gesetzen, wie z. B. der DSGVO, des BDSG oder der kommenden ePrivacy-Verordnung, sollen hier rechtliche Grenzen der Datenverarbeitung gesetzt und für Transparenz und Selbstbestimmung gesorgt werden. Auf den ersten Blick scheint dies auch zu gelingen, ist die Aufmerksamkeit für das Thema Datenschutz spätestens seit dem Inkrafttreten der DSGVO doch deutlich gestiegen. Gleichzeitig werden bei einer vertiefenden Betrachtung aber auch Spannungsfelder deutlich, deren Ursprung aus verschiedenen Sachverhalten herrühren.

Anonymisierung von Daten

Ein Ausgangspunkt können zum Beispiel die unterschiedlichen Interessen der sich gegenüberstehenden Parteien im Beschäftigungskontext sein, die je nach Perspektive zu einer positiven oder negativen Konnotation eines Technologieeinsatzes führen. Einerseits sehen Arbeitgeber das Potenzial, durch die Erhebung und Verarbeitung von Daten, die fallweise auch Rückschlüsse auf Personen ermöglichen können, ihre Prozesse effizienter zu gestalten und die Zukunftsfähigkeit ihres Unternehmens – inklusive der Arbeitsplätze – zu stärken. Aus Sicht der Beschäftigten besteht andererseits die Gefahr einer unzulässigen Kontrolle und Überwachung der Arbeitsleistungen, die zu negativen Konsequenzen für sie führen kann.

Eine Möglichkeit, den Befürchtungen sowie der Skepsis der Beschäftigten entgegenzukommen, bietet die Anonymisierung von Daten (vgl. Abschnitt 3). Mit Hilfe spezifischer Algorithmen können die erhobenen Daten derart verändert werden, dass ein Rückschluss auf einzelne Personen nicht mehr möglich ist. Folglich greifen die von den Unternehmen als kompliziert empfundenen Regelungen der DSGVO nicht mehr, woraus auf den ersten Blick ein Vorteil für die Datenverarbeitung auf Seiten der Arbeitgeber entsteht. Bei näherer Betrach-

34 Vgl. Riesenhuber, Art. 88 DSGVO, Datenschutzrecht, Wolff/Brink (Hrsg.), 37 Ed., Rn. 15 ff.
35 Vgl. Zöll, § 26 BDSG in DSGVO BDSG, Taeger/Gabel (Hrsg.), 3. Aufl. 2019, Rn. 12 ff.
36 Vgl. Franzen, BDSG § 26: in Erfurter Kommentar zum Arbeitsrecht, Müller-Glöge/Preis/Schmidt (Hrsg), 21. Aufl., 2021, Rn. 4 ff.
37 Vgl. Dietrich/Bosse/Schmitt, Kontrolle und Überwachung von Beschäftigen, DuD, 1/2021, S. 8 ff.
38 Vgl. Zöll, a.a.O., Rn. 3; eine kritischere Sicht hierzu wird vertreten von Maschmann, BDSG § 26: in DS-GVO BDSG, Kühling/Buchner (Hsrg.), 3. Aufl. 2020, Rn. 2.
39 Vgl. Bosse et al., a.a.O. S. 178.
40 Vgl. hierzu etwa die Projekte TrUSD und D'accord unter Beteiligung der Autoren dieses Beitrags.
41 Vgl. Erwägungsgrund 51 DSGVO.

tung wird jedoch klar, dass solche Verfahren nicht auf alle Datentypen anwendbar sind oder die Anonymisierung zu einem Informationsverlust führt, wodurch die Ergebnisse der Datenverarbeitung eventuell nicht mehr aussagekräftig sein können. In manchen Fällen wird eine sinnvolle Nutzung der anonymisierten Daten sogar unmöglich. Zudem kann die Skepsis bei den Arbeitnehmern bzw. Arbeitnehmervertretern bestehen bleiben, sind die Verfahren der Anonymisierung für viele Laien doch nur eine „Black Box". Ein Verständnis dafür zu schaffen, in welcher Art und Weise personenbezogene Daten systematisch verändert werden und ob nicht doch Möglichkeiten bestehen, die Daten bspw. durch De-Anonymisierung erneut auswertbar zu machen, ist im unternehmerischen Alltag nur schwerlich umsetzbar.

Eine mögliche Abhilfe könnte eine übergeordnete bzw. unabhängige Instanz sein, die mit Expertenwissen die angewandten Anonymisierungsverfahren begutachtet und entsprechende Prüfsiegel oder Zertifikate verleiht. Eine solche Instanz und ein vertrauensvolles Prüfsiegel existieren zum aktuellen Zeitpunkt jedoch nicht und könnten letztendlich auch nur schwerlich nachweisen, dass in der Praxis jegliche Möglichkeiten eines Personenbezugs in der Datenverarbeitung sowohl heute als auch mit einem zukünftigen Stand der Technik ausgeschlossen sind.

Einwilligung

Da eine Anonymisierung personenbezogener Daten nicht in allen Fällen technisch möglich oder für ein Unternehmen zielführend umsetzbar ist, bedarf es neben technischen und organisatorischen Maßnahmen (Art. 25 DSGVO) eines weiteren Instruments, um die informationelle Selbstbestimmung durchzusetzen bzw. die Verarbeitung von personenbezogenen Daten im Beschäftigungskontext rechtmäßig umzusetzen. Dies findet sich in der Einwilligung (vgl. Abschnitt 4). Direkter als die persönliche Bestätigung des Willens des Betroffenen, die auf einer bewussten Entscheidung aus freien Stücken beruht, kann eine individuelle Selbstbestimmung nicht sein.[42] Bei der Umsetzung in der Unternehmenspraxis ergeben sich jedoch organisatorische Herausforderungen und rechtliche Anforderungen an die Einwilligung. Jeden Beschäftigten einzeln um Einwilligung zu bitten und diese zu dokumentieren, kann je nach Betriebsgröße zu einem nicht zu unterschätzenden Aufwand führen – selbst wenn entsprechende Hilfsmittel eingesetzt werden, die bei der Verwaltung der Einwilligungen unterstützen und für Transparenz und Selbstbestimmung sorgen. Gleichzeitig begibt sich der Arbeitgeber in eine Abhängigkeit von der Einwilligungsbereitschaft seiner Beschäftigten, die einzeln über die Freigabe ihrer Daten zur Verarbeitung entscheiden. Das bedeutet, der Arbeitgeber hat keinerlei Garantie dafür, dass er die vorhandenen Daten einheitlich oder zumindest fallweise verarbeiten darf. Hier einen Überblick zu behalten, ist für beide Seiten mehr als schwierig, obgleich der Arbeitgeber rechtlich gesehen eine Auskunft über die Einwilligungen sowie die Verarbeitung von personenbezogenen Daten geben können und ebenfalls einen Widerruf der Einwilligung ermöglichen muss.

Auch wenn die Einwilligung des datenschutzrechtlich Betroffenen gewisse Vorteile mit sich bringt, birgt sie insbesondere im Beschäftigtenkontext aufgrund der hier geforderten Freiwilligkeit eine besondere Problematik (vgl. Abschnitt 4). Nicht nur das Machtgefälle zwischen Arbeitgeber und Arbeitnehmer bzw. Vorgesetzten und Beschäftigten kann die Ursache dafür sein, dass eine gewisse Skepsis bezüglich der Freiwilligkeit bei der Einwilligung zur Datenverarbeitung im Arbeitsverhältnis vorherrscht, auch soziale Verflechtungen oder Gruppierungen im Unternehmen können Druck auf die Entscheidungsfindung Einzelner ausüben. Dies führt dazu, dass bei einer juristischen Beurteilung der Freiwilligkeit der Einwilligung immer die bestehenden Abhängigkeiten im Beschäftigungsverhältnis sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu betrachten sind. Insgesamt muss gewährleistet sein, dass die Interessen beider Parteien gleich gelagert sind oder ein rechtlicher bzw. wirtschaftlicher Vorteil für die Beschäftigten erreicht wird.

[42] Vgl. Richter, Die Einwilligung, immer noch Zukunftsmodell? Privacy in Germany, Ausgabe 01/2018, 2018, S. 6–7.

Eine Möglichkeit das Vorgehen zu vereinfachen, ist der Abschluss einer Betriebsvereinbarung zwischen Arbeitgeber und dem Betriebsrat, der stellvertretend für alle Beschäftigten agiert. In ihr werden transparente Regelungen bezüglich spezifischer Maßnahmen zur Datenverarbeitung getroffen, die einheitlich für alle Beschäftigten gelten. Entsprechend entfällt damit aus datenschutzrechtlicher Sicht für den Arbeitgeber die Pflicht, jeden Beschäftigten im Unternehmen einzeln zu fragen. Außerdem muss der Arbeitgeber nicht befürchten, dass durch den Widerruf von Einwilligungen durch einzelne Beschäftigte eine Art Flickenteppich entsteht und fallweise eine differenzierte Betrachtung und Auswertung der Daten notwendig wird. Doch es wird häufig moniert, dass allgemeine Betriebsvereinbarungen nicht zur Sensibilisierung oder zum Verständnis bezüglich der Verarbeitung personenbezogener Daten im Unternehmen beitragen.

Handlungsempfehlung zur Abwägung

Sowohl die Anonymisierung von Daten als auch die Einwilligung zur Datenverarbeitung auf individueller Basis oder über eine Betriebsvereinbarung haben je nach zu betrachtendem Fall ihre Vor- und Nachteile. Dies verdeutlicht bereits, dass jeder Fall in der unternehmerischen Praxis einzeln betrachtet werden muss. Im Folgenden wird ein schrittweises Vorgehen zur Abwägung der verschiedenen Vor- und Nachteile vorgeschlagen, dass das oben beschriebene Beispiel einer Auswertung von Bewegungsdaten von Fahrzeugen aufgreift. Dabei wird davon ausgegangen, dass die Verarbeitung der Daten für den wirtschaftlichen Erfolg des Unternehmens relevant, aber nicht für die Erfüllung der beruflichen Tätigkeit des Beschäftigten notwendig ist.

Zunächst gilt es zu definieren, um welche Art von Daten bzw. um welche Datenklassen es sich handelt. Dies kann bereits Hinweise darauf liefern, ob eine Anonymisierung und, falls ja, welche Methode möglich und sinnvoll ist oder ob bei besonders sensiblen Daten gegebenenfalls eine individuelle Einwilligung des Datensubjekts notwendig ist. Im Beispiel aus Abschnitt 2 handelt es sich um Bewegungsdaten der Firmenfahrzeuge, die mit Hilfe von GPS-Ortungssystemen zur Positionsbestimmung erhoben werden können. Durch ein entsprechendes Vorgehen können sowohl die Kommunikation zwischen den Geräten der Arbeitnehmer und des Arbeitgebers als auch die Sensordaten selbst anonymisiert werden. Diese weitreichende Anonymisierung der Fahrzeugroutenüberwachung kann jedoch Einschränkungen in der Anwendbarkeit der Daten mit sich bringen und wäre demnach kein sinnvolles Vorgehen.

Im nächsten Schritt ist daher zu prüfen, ob die Datenklasse durch einen datenschutzrechtlichen Erlaubnistatbestand (vgl. Abschnitt 4) abgedeckt wird. Bei der Einwilligung ist an die besonderen Anforderungen im Beschäftigungskontext zu erinnern, welche eine Freiwilligkeit verlangt und daher rechtliche oder wirtschaftliche Vorteile für den Beschäftigten bzw. gleichgelagerte Interessen voraussetzt. Aufgrund des oftmals fehlenden Vorteils für die Beschäftigten und der Abhängigkeit von ihrer Einwilligungsbereitschaft sollten die anderen Erlaubnistatbestände der Einwilligung vorgezogen werden. Diese Einwilligung ist in schriftlicher oder in elektronischer Form zu dokumentieren.[43] Hierfür bietet sich der nachfolgend beschriebene Einsatz eines Privacy-Dashboards als technisches Hilfsmittel für den rechtskonformen Datenschutz im Unternehmen an.

Privacy-Dashboards als Hilfsmittel in der Unternehmenspraxis

Um den Aufwand auf Seiten der Arbeitgeber handhabbar zu halten, bieten sich digitale Hilfsmittel an, wie sie beispielsweise in Form von Privacy-Dashboards umgesetzt werden können. Diese unterstützen insbesondere dabei, Transparenz und Selbstbestimmung bei der Verarbeitung der personenbezogenen im Unternehmen zu gewährleisten und rechtskonform umzusetzen. So können beispielsweise zweckgebunden konkrete Daten für die Verarbeitung angefragt und einzeln durch den betroffenen Beschäftigten freigegeben werden. Zudem wird

[43] Vgl. Franzen, § 26 BDSG, in Erfurter Kommentar zum Arbeitsrecht, Müller-Glöge/Preis/Schmidt (Hrsg.), 21. Aufl., 2021, Rn. 43 ff; mit Spannung zu Verfolgen sind in diesem Zusammenhang auch die neuen Entwicklungen durch Einführung des Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) insbesondere mit Hinblick auf die „Personal Information Management Services" (PIMS) des § 26 TTDSG.

mit Hilfe eines Privacy-Dashboards ersichtlich, welche Daten zu welchem Zweck bereits verarbeitet werden. Dies ermöglicht gleichzeitig einen schnellen und problemlosen Widerruf der Einwilligung zur zweckgebundenen Datenverarbeitung, insofern der Beschäftigte davon Gebrauch machen will. Jedoch bleibt ungeachtet eines technologiegestützten Einwilligungsmanagement mit Hilfe eines Privacy-Dashboards die Verantwortung beim Unternehmen, die Rechtskonformität mit der DSGVO, bspw. Datenminimierung, zu gewährleisten.

6. Zusammenfassung und Fazit

Durch die zunehmende Digitalisierung der Arbeitswelt steigen auch die Möglichkeiten, durch Datenverarbeitungen Unternehmensprozesse zu optimieren oder frühzeitig Gesundheitsbelastungen für Beschäftigte zu erkennen. Verarbeitungen personenbezogener Daten unterliegen jedoch dem Schutz der DSGVO und des BDSG. Diese erlauben das Verarbeiten einer begrenzten Teilmenge der definierten personenbezogenen Datenklassen durch konkrete Erlaubnistatbestände. Viele Verarbeitungen personenbezogener Daten bedürfen jedoch der Einwilligung der Beschäftigten. Diese Einwilligung ist im Beschäftigungsverhältnis umstritten.

Eine Alternative ist die Anonymisierung personenbezogener Daten, die zur Folge hat, dass der Personenbezug entfernt wird und die Daten nicht mehr in den Anwendungsbereich von DSGVO und BDSG fallen. Anonymisierungsmethoden bringen jedoch Einschränkungen mit sich, weshalb sie nicht auf alle Datentypen anwendbar sind. Hinzu kommt, dass es für eine sinnvolle Nutzung nicht immer möglich ist, Daten zu anonymisieren.

Als Empfehlung für die Planung notwendiger Datenverarbeitungen personenbezogener Daten schlagen wir ein schrittweises Vorgehen vor: Zuerst sollte die Datenklasse der gewünschten Daten analysiert werden (Schritt 1) und anschließend geprüft werden, ob eine Anonymisierung der Daten inhaltlich und technisch möglich ist (Schritt 2). Ist dies nicht der Fall, so ist zu prüfen, ob es einen Erlaubnistatbestand gibt, der diese Verarbeitung erlaubt (Schritt 3), wobei die Einwilligung möglichst vermieden werden sollte. Dieses Vorgehen kann es Unternehmen erleichtern, einen passenden Rahmen für die rechtskonforme Nutzung personenbezogener Daten zu finden und somit mehr Sicherheit in der Verarbeitung von personenbezogenen Daten zu erhalten.

7. Danksagung

Diese Arbeit wurde durch das Forschungsprojekt „D'accord – Adaptive Datenschutz-Cockpits in digitalen Ökosystemen“ unterstützt, finanziert durch das Bundesministerium für Bildung und Forschung (BMBF).