Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen

baua: Bericht

baua
Bundesanstalt für Arbeitsschutz
und Arbeitsmedizin

Forschung
Projekt F 2412

B. Varadinek
M. Indenhuck
E. Surowiecki

Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen

1. Auflage 2018
Dortmund/Berlin/Dresden

Diese Veröffentlichung beruht auf dem Gutachten „Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen“ im Auftrag der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. Es wurde erstellt, um u .a. die Arbeiten im Forschungsprojekt F 2412 „Interaktive personalisierte Visualisierung in Industrieprozessen am Beispiel der Digitalen Fabrik in der Elektronik-Fertigung (Glass@Service)“ zu ergänzen. Das Projekt Glass@Service wird mit Mitteln des Bundesministeriums für Wirtschaft und Energie in der Fördermaßnahme „Entwicklung konvergente IKT“ gefördert und vom Projektträger Deutsches Zentrum für Luft- und Raumfahrt betreut (Förderkennzeichen: 01MD16008B).
Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Autoren: Dr. Brigitta Varadinek, Maître en droit
Dr. Moritz Indenhuck
Eva Surowiecki, LL.B.
Lindenpartners Partnerschaft von Rechtsanwälte mbB
Friedrichstr. 95, 10117 Berlin

Fachliche Begleitung: Jan Terhoeven
Dr. Sascha Wischniewski
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin

Titelfoto: Wavebreak/iStock.com

Umschlaggestaltung: Vanessa Seeger
Bundesanstalt für Arbeitsschutz und Arbeitsmedizin

Herausgeber: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA)
Friedrich-Henkel-Weg 1 – 25, 44149 Dortmund
Postanschrift: Postfach 17 02 02, 44061 Dortmund
Telefon 0231 9071-2071
Telefax 0231 9071-2070
E-Mail *info-zentrum@baua.bund.de*
Internet *www.baua.de*

Berlin: Nöldnerstraße 40 – 42, 10317 Berlin
Telefon 030 51548-0
Telefax 030 51548-4170

Dresden: Fabricestraße 8, 01099 Dresden
Telefon 0351 5639-50
Telefax 0351 5639-5210

doi:10.21934/baua:bericht20180820 (online)

www.baua.de/dok/8754472

Inhaltsverzeichnis

Rechtliche Anforderungen an den Datenschutz bei adaptiven Arbeitsassistenzsystemen

Kurzreferat

Adaptive Arbeitsassistenzsysteme sind durch zwei Entwicklungen gekennzeichnet: zum einen erlaubt der technische Fortschritt eine immer stärkere und diversifiziertere Anwendung in vielen Industriebereichen. Zum anderen wurde das Datenschutzrecht durch die Datenschutzgrundverordnung (DSGVO) europaweit auf eine neue rechtliche Grundlage gestellt und setzt so einen neuen Rahmen für den Einsatz dieser Systeme. Beide Entwicklungen sind Anlass einer vertieften Befassung mit den datenschutzrechtlichen Anforderungen an den Einsatz von Arbeitsassistenzsystemen im Unternehmen. Dabei konnten folgende wesentliche Erkenntnisse gewonnen werden:

- Die mit dem Einsatz von adaptiven Assistenzsystemen einhergehende Verarbeitung von Beschäftigtendaten wird regelmäßig durch § 26 Abs. 1 BDSG-neu, Verarbeitung im Rahmen des Beschäftigtenverhältnisses, gedeckt sein.
- Der Einsatz von adaptiven Assistenzsystemen kann auch durch eine Kollektivvereinbarung geregelt werden.
- Die Einwilligung des Beschäftigten wird demgegenüber nur in Ausnahmefällen in Betracht kommen.
- Die jeweilige Datenverarbeitung muss für einen bestimmten Zweck im Interesse des Unternehmers erforderlich sein. Zweckänderungen sind in Grenzen durch die DSGVO zulässig. Das unspezifische Sammeln von Beschäftigtendaten im Rahmen einer gläsernen Fabrik ist demgegenüber nicht zulässig.
- Dem Beschäftigten stehen umfangreiche Betroffenenrechte zur Seite. Dazu zählen Informations- und Auskunftsansprüche, das Recht auf Berichtigung und Löschung und das Recht auf Datenportabilität. Grenzen dieser Ansprüche sind im Zusammenhang mit adaptiven Assistenzsystemen jedoch die Unternehmerinteressen, insb. Geschäfts- und Betriebsgeheimnisse.
- Die DSGVO verstärkt den technischen Datenschutz. Gerade auch bei adaptiven Assistenzsystemen ist daher zu prüfen, ob durch Technikgestaltung, datenschutzrechtliche Voreinstellungen und Anonymisierungs- oder Pseudonymisierungskonzepte der Eingriff in das Persönlichkeitsrecht der Beschäftigten durch die Datenverarbeitung vermieden oder abgemildert werden kann.

Schlagwörter:

Adaptive Arbeitsassistenzsysteme, Allgemeine Datenschutzbestimmungen, DSGVO, Datenschutz, Datenübertragbarkeit, persönliche Daten, Mitarbeiter, Unternehmen, Anonymisierungskonzepte, Pseudonymisierungskonzepte, Informationsrechte, Datensubjektrechte

Data protection requirements for the application of adaptive work assistance systems

Abstract

Adaptive work assistance systems are characterized by two developments: On the one hand, the progress in technology allows for an increasingly stronger and more diversified application in many industrial sectors. On the other hand, the General Data Protection Regulation (GDPR) established a new legal standard for data protection law in Europe which sets a new framework for the application of these systems. Both developments give reason to focus more deeply on data protection requirements for the application of work assistance systems in companies. The following key points have resulted from the analysis:

- The application of adaptive assistance systems and the corresponding processing of employees' personal data will generally be covered by section 26 (1) Federal Data Protection Act (BDSG-neu) on data processing for employment-related purposes.
- The application of adaptive assistance systems can also be regulated by collective agreements.
- The employee´s consent, on the other hand will, only come into consideration in exceptional cases be a viable option.
- The data processing in question must be necessary for a specific purpose. Amendments to the purpose are only admissible within very narrow limits of the GDPR. By contrast, collecting employees' personal data without specifying the purpose similar to a "glass factory", is prohibited.
- Employees have comprehensive data subject rights, including the rights of information, access to and rectification or erasure of personal data as well as the right to data portability. In connection with adaptive assistance systems, these rights can however be limited by interests of the company, in particular trade and business secrets.
- The GDPR strengthens technical data protection. Especially concerning adaptive assistance systems, it is necessary to verify whether restricting on the employees' privacy through data processing can be avoided or mitigated by appropriate technical measures, default setting in terms of data minimisation and anonymization or pseudonymization concepts.

Key words:

Adaptive work assistance systems, General Data Protection Regulation, GDPR, data protection, data portability, personal data, employee, company, anonymization concepts, pseudonymization concepts, rights of information, data subject rights

Thema und inhaltliche Beschreibung des Projekts

Trotz voranschreitender Technologisierung und zunehmendem Einsatz vernetzter Objekte mit eigener intelligenter und dezentraler Steuerung wird die menschliche Arbeit ein wesentlicher Bestandteil in Produktionsprozessen bleiben. Auf absehbare Zeit wird man Wahrnehmung, Sensorik und Entscheidungsfähigkeit des Menschen bei komplexen, nicht eindeutigen oder unvorhersehbaren Arbeitsaufgaben nicht durch die Logik einer Maschine abbilden können.[1] Adaptive Technologien können in diesem Zusammenhang – etwa durch die automatische Bereitstellung handlungsleitender Informationen – Zielorientierung und Korrektheit von menschlichem Verhalten unterstützen. Als adaptive Arbeitsassistenzsysteme werden dabei informationstechnisch vernetzte Arbeitsmittel und -systeme bezeichnet, welche die menschliche Arbeit kontextabhängig unterstützen.[2] Hierzu erheben solche Systeme verschiedene Parameter wie Position oder die Identitätsdaten, werten diese aus und verknüpfen sie mit anderen Daten. Die hierdurch gewonnen Informationen können digital aufbereitet und im Rahmen vernetzter Arbeitssysteme verfügbar gemacht werden. Durch das Assistenzsystem erhält der Nutzer Zugang zu digitalen Informationen, die er selbst ohne zusätzliche Hilfsmittel nicht wahrnehmen oder verarbeiten kann.

Als Basistechnologien gelten dabei insbesondere die Radiofrequenz-Identifikation (RFID) sowie Augmented Reality (AR). Während RFID eine eindeutige, schnelle, berührungslose und gleichzeitige Identifikation von Objekten und Personen – auch ohne direkte Sichtverbindung – ermöglicht, können Nutzer über AR-Systeme in Echtzeit mit einer um virtuelle Objekte angereicherten Umgebung interagieren. Wesentliche Bestandteile von AR-Systemen sind Head-Mounted-Displays (HMD) oder Datenbrillen, die eine mobile Darstellung relevanter Informationen unmittelbar in der jeweiligen Arbeitsumgebung ermöglichen.

Gerade im Kontext der Industrie 4.0 bietet die Verzahnung industrieller Produktion und moderner Informations- und Kommunikationstechniken zahlreiche Vorteile. Die hierdurch gewonnenen Daten können verwendet werden, um die Arbeitsumgebung durch anforderungsadäquate oder belastungsoptimale Gestaltung positiv zu beeinflussen. So können etwa Sensorsysteme eine bedarfsgerechte Beleuchtung und Klimatisierung von Arbeitsräumen ermöglichen. Zahlreiche Arbeitsprozesse können durch adaptive Arbeitsassistenzsysteme unterstützt und sicherer gestaltet werden. Ein Beispiel hierfür bietet ein vom Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF entwickeltes RFID-Armband, mit dem Objekte oder Greifbereiche in Kommissionier- oder Montageprozessen schnell und automatisch identifiziert

---

[1] *Wölfle*, Kontextsensitive Arbeitsassistenzsysteme zur Informationsbereitstellung in der Intralogistik, S. 3.

[2] Vgl. *Grötsch/Geilen u.a.*, Chancen und Herausforderungen der zunehmenden Digitalisierung in der Arbeitswelt, in: Christoph Schlick (Hg.), Arbeit in der digitalisierten Welt – Beiträge der Fachtagung des BMBF 2015, S. 83.

werden können.[3] Auch können etwa Videoaufnahmen bei der Bearbeitung von Aufgaben oder zu Trainingszwecken unterstützend eingesetzt werden.

Adaptive Assistenzsysteme eignen sich aber nicht nur zur Unterstützung bei konkret definierten Aufgaben. In dem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojekt SmartF-IT[4] realisiert die Deutsche Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) situationsadaptive Assistenzsysteme, die über eine gemeinsame Wissensbasis aktuelle Informationen über Anlagen, Produkte, Prozesse, Dienste und Beschäftigte nutzen und austauschen können. Diese Datenbasis stellt ein „integriertes semantisches Fabrikgedächtnis für multiadaptive Prozesse“ dar. Ein solches Fabrikgedächtnis kann Informationen aus den unterschiedlichen Bereichen der Produktion dynamisch miteinander verknüpfen und so die jeweils aktuelle Produktionssituation bezüglich Anlagen, Beschäftigten, Produkten und Prozessen darstellen und anwendungsübergreifend verfügbar machen. Hierzu gehören beispielsweise:

- Assistenz für Fertigungsplaner und -steuerer durch integrierte IT-Systeme und Simulation
- Assistenz für Werker durch „Guided Picking“ zur adaptiven Materialbereitstellung
- Assistenz für Teamleiter zur kooperativen Entscheidungsunterstützung bei der Personaleinsatzplanung
- Assistenz für Werker und Entscheider zum kooperativen Störungsmanagement
- Individuelle Assistenz für Werker angepasst an aktuelle Fähigkeiten und Prozessschritte

Die Anwendung „kooperativer Dienste zur Auftrags- und Personaleinsatzplanung“ soll mithilfe adaptiver Assistenzsysteme und auf Grundlage eines semantischen Fabrikgedächtnisses beispielsweise die Personaleinsatzplanung in den Produktionsbereichen unterstützen. Zu jedem Beschäftigten werden produktspezifisch die Kennzahlen Erfahrung, Produktivität und Qualität vom System mit Hilfe von Aggregierungsmechanismen gepflegt. Diese Informationen sind ausschließlich zweckgebunden für den verantwortlichen Teamleiter einsehbar. Unter den Teamleitern lassen sich systemweit Beschäftigte anfordern und vorschlagen, sodass kurzfristige Personalengpässe schnell mit Hilfe eines IT-gestützten Kollaborationsprozesses gelöst und gegebenenfalls eskaliert werden können.

Das semantische Fabrikgedächtnis stellt somit eine umfassende Datenbasis des Unternehmens dar, die Einzelanwendungen wie die Personaleinsatzplanung unterstützt.

Neben den unbestreitbaren Vorteilen müssen im Rahmen der rechtlichen Bewertung aber insbesondere auch die Risiken berücksichtigt werden, die mit dem Einsatz adaptiver Arbeitsassistenzsysteme verbunden sein können. So sind Umfang und Zweck der Datenerhebung und -verarbeitung für die Betroffenen nicht immer trans-

---

[3] Vgl. Fraunhofer-Institut für Fabrikbetrieb und -automatisierung IFF, „RFID-Armband“ zur Mobilen Objekt-Identifikation im Handlingsprozess, abrufbar unter: http://www.iff.fraunhofer.de/content/dam/iff/de/dokumente/publikationen/rfid-armband-zur-mobilen-objekt-identifikation-im-handlingprozess-fraunhofer-iff.pdf (zuletzt aufgerufen am 15. Mai 2017).

[4] SmartF-It Projekte: http://www.smartf-it-projekt.de/wp-content/uploads/SmartF-IT_HMI2016.pdf

parent. Auch können besonders sensible Daten betroffenen sein, an deren Vertraulichkeit der Beschäftigte ein besonderes Interesse hat. So können etwa über sog. Wearables heute nicht nur die Position, sondern auch Gesundheitsdaten einer Person erfasst werden.

Das größte Risiko wird aber wohl derzeit in der Erstellung vollständiger Beschäftigtenprofile und einer Dauerüberwachung von Beschäftigten gesehen. So kommt Prof. Dr. Krause in dem für das Bundesministerium für Arbeit und Soziales erstellten Forschungsbericht „Digitalisierung und Beschäftigtendatenschutz“ [5] zu dem Ergebnis, dass die Digitalisierung des Wirtschafts- und Arbeitslebens dazu führe, dass im Zusammenhang mit betrieblichen Prozessen eine immer größere Menge auch an personenbezogenen Beschäftigtendaten erhoben und ausgewertet werden. Dabei sieht Krause ein erhebliches Kontrollpotential durch die neuen technischen Entwicklungen. Um den Risiken für die Beschäftigten entgegenzuwirken, bedürfe es eines Beschäftigtendatenschutzes, der insb. heimliche Kontrollen, umfassende Bewegungsprofile, Dauerüberwachung und Persönlichkeitsdurchleuchtung für unzulässig erklärt.

Im Rahmen der rechtlichen Bewertung wurde neben dem genannten Forschungsbericht auch das vom Auftraggeber veröffentlichte Gutachten „Ergonomie im Spannungsfeld von Arbeits-, Daten- und Diskriminierungsschutz“ berücksichtigt.

[5] Forschungsbericht „Digitalisierung und Beschäftigtendatenschutz“ für das Bundesministerium für Arbeit und Soziales, erstellt von Prof. Dr. Rüdiger Krause, Georg-August-Universität Göttingen, Nov. 2016

1 Einführung

1.1 Das deutsche Datenschutzrecht und die DSGVO

In Deutschland gilt bis zum 25. Mai 2018 das Bundesdatenschutzgesetz (nachfolgend: BDSG-alt). Zentrale Vorschrift für den Beschäftigtendatenschutz ist derzeit § 32 BDSG-alt. Am 25. Mai 2018 wird die Datenschutzgrundverordnung[6] (DSGVO) in Kraft treten. Für die Verarbeitung personenbezogener Daten, ob im privaten oder öffentlichen Bereich, gilt dann überall in der EU grundsätzlich einheitlich und gleichzeitig dasselbe Recht, ohne dass es dafür noch eines weiteren nationalen Rechtsanwendungsbefehls oder Inkorporationsaktes bedarf.[7]

Allerdings enthält die DSGVO zahlreiche sog. Öffnungsklauseln, die es den Mitgliedsstaaten erlauben, nationale Vorschriften zu erlassen. Der deutsche Gesetzgeber hat hiervon Gebrauch gemacht und mit dem Gesetz zur Anpassung des Datenschutzrechts an die VO (EU) Nr. 2016/679 (DSGVO) und zur Umsetzung der RL (EU) 2016/6801 (JI-RL)2 das BDSG umfassend neu gefasst (nachfolgend BDSG-neu). Das BDSG-neu wird ebenfalls am 25. Mai 2018 in Kraft treten.

1.1.1 Die Öffnungsklausel in Art. 88 DSGVO zum Beschäftigtendatenschutz

Für den Beschäftigtendatenschutz enthält die DSGVO in Art. 88 Abs. 1 DSGVO eine Öffnungsklausel:

„Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen."

Von dieser Öffnungsklausel hat der deutsche Gesetzgeber Gebrauch gemacht und mit § 26 BDSG-neu spezifische Regelungen für die Datenverarbeitung im Beschäftigtenkontext erlassen. Die Bestimmung übernimmt weitgehend die Regelungen des

---

[6] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

[7] *Selmayr/Ehmann* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Einführung Rn. 1-8.

bisherigen § 32 BDSG-alt[8] und damit nach dem ausdrücklichen Willen des Gesetzgebers auch die hierzu von der Rechtsprechung des Bundesarbeitsgerichts (BAG) entwickelten Grundsätze.[9]

Da es aufgrund der Öffnungsklausel dem nationalen Gesetzgeber gestattet ist, eigene Vorschriften zu erlassen, geht § 26 BDSG-neu den allgemeinen Regeln der DSGVO als speziellere Vorschrift vor. Allerdings sind Einzelheiten des Verhältnisses zwischen der DSGVO und der nationalen Bereichsvorschrift noch ungeklärt. So dürfen die nationalen Gesetzgeber nach dem Wortlaut von Art. 88 Abs. 1 DSGVO lediglich „spezifischere Vorschriften" bestimmen. Dies dürfte so zu verstehen sein, dass die Vorgaben der DSGVO den „Mindeststandard" für den Beschäftigtendatenschutz darstellen. Unter diesen darf der nationale Gesetzgeber das Datenschutzniveau für die Beschäftigte nicht herabsetzen, sondern nur Konkretisierungen vornehmen. Überwiegend wird zudem angenommen, dass der Gesetzgeber im Rahmen der nationalen Umsetzung Abweichungen „nach oben", also strengere Vorschriften vorsehen darf.[10]

Zu den Grundregeln aus der DSGVO, von denen der nationale Gesetzgeber nicht abweichen darf, sollen folgende Vorschriften zählen[11]:

- Art. 5 DSGVO, der die allgemeinen Verarbeitungsgrundsätze[12] festlegt,
- Art. 6 DSGVO über die Rechtmäßigkeit der Verarbeitung,
- Art. 7 DSGVO über die Anforderungen an eine Einwilligung,
- Art. 15 DSGVO über die Betroffenenrechte.

Eine weitere, inhaltliche Schranke setzt Art. 88 Abs. 2 DSGVO. Die unter Art. 88 DSGVO erlassenen Vorschriften müssen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz. Dieser Katalog ist zwar nicht abschließend, gleichwohl dürfte dieser als Richtschnur für eine Auslegung der nationalen Gesetzgebung dienen.

§ 26 BDSG-neu hält sich innerhalb dieser von der DSGVO vorgegebenen Grenzen.[13] Aber auch die Anwendung des § 26 BDSG-neu hat in Einklang mit den oben ge-

---

[8] Neu ist, dass mit § 26 Abs. 2 BDSG-neu nun erstmals auch Vorgaben für die Einwilligung im Beschäftigungsverhältnis ausdrücklich geregelt sind. Zudem wird die derzeitige Praxis zur Regelung datenschutzrechtlicher Fragen in Kollektivvereinbarung durch § 26 Abs. 4 BDSG-neu künftig auf eine ausdrückliche Rechtsgrundlage gestellt, vgl. hierzu *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, Art. 88 DSGVO Rn. 100.

[9] BT-Drucks. 16/13657, S. 35; *Gola*, Die EU DS-GVO und der Beschäftigungsdatenschutz – Was bleibt und was ist neu?, GDD

[10] *Imping*, CR 2017, 378 (379), Neue Zeitrechnung im (Beschäftigten-)Datenschutz, m.w.N.

[11] *Düwell/Brink*, NZA 2016, 665 (667), Die EU- DS-GVO und der Beschäftigtendatenschutz.

[12] Vgl. hiernach C.II

[13] Vgl. nur *Gola/Thüsing/Schmidt*, DuD 2017, 244 (249), Was wird aus dem Beschäftigtendatenschutz?

nannten Grundregeln der DSGVO zu erfolgen. Es ist zu erwarten, dass der Europäische Gerichtshof (EuGH) diese allgemeinen Grundsätze weiter konkretisieren und damit auch auf den Beschäftigtendatenschutz Einfluss nehmen wird.

1.1.2 Weitere Rechtsgrundlagen für die Datenverarbeitung

§ 26 Abs. 1 Satz BDSG-neu ermöglicht die Verarbeitung personenbezogener Daten „für die Zwecke des Beschäftigungsverhältnisses“. Die Regelung enthält damit die zentrale Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten. Daneben kommen allerdings weitere Verarbeitungsgrundlagen in Betracht. So gelten die Bestimmungen der DSGVO unmittelbar, soweit die Mitgliedsstaaten keine spezifischen Regelungen zum Beschäftigtendatenschutz erlassen haben oder soweit kein „Beschäftigtenkontext“ vorliegt.[14] Werden etwa Personaldaten für andere als in § 26 BDSG-neu genannte Zwecke, d.h. für sog. Beschäftigungsfremde Zwecke verarbeitet, kann auf die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DSGVO zurückgegriffen werden.[15]

Art. 6 Abs. 1 lit. c DSGVO erlaubt darüber hinaus die Datenverarbeitung in Erfüllung einer rechtlichen Verpflichtung. Voraussetzung ist, dass die Rechtsgrundlage einen bestimmten Datenverarbeitungsvorgang anordnet.[16] Im Zusammenhang mit adaptiven Assistenzsystemen dürfte Art. 6 Abs. 1 lit. c DSGVO nur selten zur Anwendung kommen. Zwar ist es denkbar, dass der Arbeitgeber solche Systeme (auch) einsetzt, um etwa gesetzliche Vorgaben des Arbeitsschutzes zu erfüllen. Mit Blick auf das Arbeitsschutzgesetz (ArbSchG) hat Thüsing[17] allerdings mit überzeugender Begründung dargelegt, dass der Gesetzgeber nur selten konkrete Schutzmaßnahmen vorgibt. In der Regel steht dem Arbeitgeber Ermessen zu, wie er das Arbeitsschutzrecht umsetzt. Das ArbSchG und verwandte Rechtsvorschriften enthalten daher in aller Regel keine Pflicht zur Datenverarbeitung und können somit nicht als Rechtsgrundlage herangezogen werden. Erfolgt die Verarbeitung von Beschäftigtendaten zum Zwecke des Arbeitsschutzes oder anderer gesetzlicher Vorgaben, kann dies allerdings im Rahmen der Interessenabwägung berücksichtigt werden.[18]

Die DSGVO und das BDSG-neu sehen zudem die Möglichkeit vor, im Rahmen von Kollektivvereinbarungen spezifische Vorschriften zum Beschäftigtendatenschutzrecht schaffen.[19]

Wie bisher, kann die Verarbeitung von Beschäftigtendaten zudem durch die Einwilligung der Betroffenen nach Art. 7 DSGVO und § 26 Abs. 2 BDSG-neu gerechtfertigt sein.[20]

---

[14] *Imping*, CR 2017, 378 (379), Neue Zeitrechnung im (Beschäftigten-)Datenschutz?
[15] Vgl. hiernach D.II.
[16] *Albers,* in: Wolff/Brink BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 6 DSGVO Rn. 35.
[17] Thüsing, Ergonomie im Spannungsfeld von Arbeits-, Daten- und Diskriminierungsschutz, Gutachten für BAUA, 2014.
[18] Thüsing, a.a.O. S. 53.
[19] Vgl. hiernach D.III.
[20] Vgl. hiernach D.IV.

1.2 Allgemeine Datenschutzgrundsätze

Neben der Rechtfertigungsgrundlage für die Datenverarbeitung müssen bei der Beurteilung der Verarbeitung personenbezogener Daten im Zusammenhang mit adaptiven Assistenzsystemen zahlreiche weitere Vorschriften beachtet werden, die sich aus einem Zusammenspiel der vorrangig geltenden DSGVO und den zur Umsetzung erlassenen deutschen Normen des BDSG-neu ergeben.

Zu den zu beachtenden Vorschriften gelten an erster Stelle die allgemeinen Datenschutzgrundsätze gemäß Art. 5 DSGVO. Diese Datenschutzgrundsätze konkretisieren das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung und sind daher bei der Auslegung der konkreten Regelungen heranzuziehen. Bei der Frage der Zulässigkeit der Datenverarbeitung im Zusammenhang mit adaptiven Assistenzsystemen wird man regelmäßig auf diese allgemeinen Datenschutzgrundsätze zurückgreifen müssen, da die gesetzlichen Rechtfertigungsgründe keine konkreten Aussagen zu diesen neuen Technologien und den damit verbundenen Fragestellungen treffen. Der Gesetzgeber, der das BDSG-neu technikneutral gestalten wollte, hat bisher darauf verzichtet, mit Blick auf neuartige Datenverarbeitungsvorgänge, die mit der zunehmenden Digitalisierung des Beschäftigtenumfeldes einhergehen, gesonderte Regelungen zu schaffen.[21] Dieser offene Regelungsansatz bietet den Vorteil, dass auch neue Entwicklungen anhand allgemeiner Grundsätze und der relativ allgemein gehaltenen Rechtfertigungsgrundlage in § 26 BDSG-neu beurteilt werden können. Allerdings geschieht dies auf Kosten der Rechtssicherheit: Viele Gerichte und Aufsichtsbehörden beginnen gerade erst, sich näher mit der Digitalisierung der Arbeitswelt zu befassen und auch die rechtswissenschaftliche Behandlung dieses Themas steckt noch in den Anfängen. Vor diesem Hintergrund lässt sich häufig nur schwer prognostizieren, wie die juristische Praxis die zahlreichen Wertungsspielräume der DSGVO und des BDSG-neu ausfüllen wird.

1.2.1 Grundsatz der Rechtmäßigkeit der Datenverarbeitung

Nach Art. 5 Abs. 1 lit. a DSGVO müssen Daten rechtmäßig verarbeitet werden. Dieser Grundsatz der Rechtmäßigkeit der Verarbeitung wird in Art. 6 Abs. 1 DSGVO dahingehend konkretisiert, dass eine Datenverarbeitung nur zulässig ist, wenn sie auf einer Einwilligung oder auf einem der sonstigen in Art. 6 Abs. 1 lit. b bis f DSGVO genannten Rechtfertigungsgründe beruht. Auch unter der DSGVO gilt damit – wie schon unter dem BDSG-alt – das Konzept des Verbots mit Erlaubnisvorbehalt.

Nachfolgend[22] werden daher die für die Datenverarbeitung bei adaptiven Assistenzsystemen in Betracht kommenden Rechtfertigungsgründe genauer begutachtet:

- Verarbeitung für die Zwecke des Beschäftigungsverhältnisses, § 26 BDSG-neu,
- Verarbeitung auf Grundlage einer Interessenabwägung, Art. 6 Abs. 1 lit f DSGVO,

---

[21] Beispielhaft sei auf die Anregungen zum legislativen Fortentwicklungsbedarf im Forschungsbericht „Digitalisierung und Beschäftigtendatenschutz, Seite 48 ff. verwiesen. Der Gesetzgeber hat bisher einen eigenständigen Beschäftigtendatenschutz, wie vielfach gefordert, nicht erlassen.

[22] Hiernach Gliederungspunkt D.

- Verarbeitung auf Grundlage einer Einwilligung des Betroffenen, Art. 7 DSGVO, § 26 Abs. 2 Satz 1 BDSG-neu,
- Verarbeitung auf Grundlage einer Kollektivvereinbarung, § 26 Abs. 4 Satz 1 BDSG-neu.

Die Verarbeitung zum Zwecke der Vertragserfüllung gemäß Art. 6 Abs. 1 lit. b wird von § 26 BDSG-neu verdrängt, so dass diese Rechtfertigung vorliegend keine Rolle spielt. Auch Art. 6 Abs. 1 lit c DSGVO, der die Verarbeitung erlaubt, wenn sie in Erfüllung einer rechtlichen Verpflichtung erfolgt, dürfte im Zusammenhang mit adaptiven Assistenzsystemen allenfalls eine untergeordnete Rolle spielen.[23]

1.2.2 Verarbeitung nach dem Grundsatz von Treu und Glauben

Daten müssen gemäß Art. 5 Abs. 1 lit a DSGVO nach dem Grundsatz von Treu und Glauben verarbeitet werden. Dieser Grundsatz lässt sich als ein Fairnessgebot verstehen. Bei Arbeitsverträgen ergibt sich der Grundsatz bereits aus § 242 BGB.

1.2.3 Transparenzgrundsatz

Gem. Art. 5 Abs. 1 lit. a DSGVO muss die Datenverarbeitung in einer für den Betroffenen nachvollziehbaren Weise erfolgen. Der Grundsatz der Transparenz wird insb. in den Informationspflichten in Art. 12 bis 14 DSGVO näher konkretisiert, die deutlich über die nach dem BDSG geregelten Benachrichtigungs- und Informationspflichten hinausgehen.[24] Dieser Grundsatz spielt bei der Anwendung adaptiver Assistenzsysteme eine zentrale Rolle. Aufgrund der technischen Komplexität der Datennutzung und der nicht ohne weiteres erkennbaren Risiken, die aus einer Vernetzung verschiedener Systeme resultieren können, müssen dem Beschäftigten transparente Informationen zur Verfügung gestellt werden, um seine Persönlichkeitsrechte zu wahren.

Der Grundsatz der Transparenz umfasst neben den Informationspflichten auch den Auskunftsanspruch in Art. 15 DSGVO und die Berichtspflicht der Datenschutzaufsicht (Art. 59 DSGVO).

1.2.4 Grundsatz der Zweckbindung

Gem. Art. 5 Abs. 1 lit. b DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.

Wie bereits nach dem geltenden BDSG muss der konkrete Zweck bei Erhebung der personenbezogenen Daten festgelegt sein. Mit diesem Grundsatz sind Überlegungen zur vollständig vernetzten Industrie 4.0, bei der Daten in jeder Produktionsphase gesammelt werden, um hieraus Erkenntnisse zur Optimierung von Produktionsabläufen, zum Einsatz von Maschinen und Beschäftigten, zur Weiterentwicklung von Produkten usw. abzuleiten, nur schwer zu vereinbaren. Das „semantische Fabrikgedächtnis“ beispielsweise sammelt eine Vielzahl von Daten, die zu den verschiedens-

---

[23] Vgl. Gutachten Thüsing, S. 51 ff. sowie oben, I.2.
[24] Vgl. hierzu näher Gliederungspunkt E.

ten Zwecken erhoben wurden und die anschließend für verschiedenste – im Zeitpunkt der Erhebung häufig noch nicht feststehende – Zwecke genutzt werden sollen. Die Erstellung einer allgemeinen Datenbasis für nicht definierte Zwecke ist unzulässig. Es dürfen keine Daten ohne konkreten Zweck erhoben und gespeichert werden, um dann anhand daraus abgeleiteter Muster und Algorithmen den konkreten Nutzen zu bestimmen. Eine derartige Datenbank ist allein mit anonymisierten Daten und reinen Produktionsdaten, nicht aber mit auf einzelne Beschäftigte rückführbare Daten zulässig.

Allerdings ist eine Zweckänderung, anders als noch unter dem BDSG-alt, im Verlauf der Verarbeitung nunmehr ausdrücklich zulässig, wenngleich unter engen Voraussetzungen.[25] Entscheidend ist die Kompatibilität des neuen Zwecks mit dem alten Zweck gemäß Art. 6 Abs. 4 DSGVO (sog. Kompatibilitätstest). Eine Weiterverarbeitung zu einem anderen Zweck als bei der Datenerhebung festgelegt ist bei Kompatibilität der Zwecke auch ohne neue Rechtsgrundlage, wie beispielsweise einer Einwilligung, zulässig.[26] Maßgeblich für die Beurteilung der Kompatibilität ist vor allem die Erwartungshaltung des Beschäftigten, d.h. ob er bei Erhebung der Daten mit der Nutzung zu diesem „neuen“ Zweck rechnen konnte. Daneben ist auch darauf abzustellen, ob die Verarbeitung in Folge der Zweckänderung zu einem intensiveren Eingriff in das Recht auf informationelle Selbstbestimmung des Beschäftigten führt. Kommt es zu einer Zweckänderung ist zudem der Transparenzgrundsatz zu beachten und der Betroffene gem. Art. 13 Abs. 3 bzw. 14 Abs. 4 DSGVO vorab entsprechend zu informieren.

Diese durch die DSGVO geschaffene Möglichkeit der Zweckänderung könnte bei der Datenverarbeitung im Rahmen adaptiver Assistenzsysteme eine wichtige Rolle spielen. So ist es beispielsweise denkbar, dass aus den Daten, die im Rahmen des „Guided Picking“ zur adaptiven Materialbereitstellung erhoben werden, Erkenntnisse gewonnen werden, die auch für Beschäftigteneinsatzplanung genutzt werden könnten. Eine derartige Zweckänderung dürfte zulässig sein, da die Zwecke kompatibel sind. Weiß der Beschäftigte, dass seine Daten im Rahmen des „Guided Picking“ zur Verbesserung der einzelnen Arbeitsabläufe verwendet werden, so kann der Beschäftigte erwarten, dass diese Daten auch in anderen Systemen zur Verbesserung der Arbeitsorganisation verwendet werden. Da die Interessenlage in beiden Fällen vergleichbar ist, handelt es sich aus Sicht des Beschäftigten nicht um eine völlig andere Verwendungskategorie.

Sollten diese Daten hingegen genutzt werden, um Beschäftigtenprofile zu erstellen oder Leistungskontrollsysteme einzuführen, wäre diese Zweckänderung nicht zulässig. Diese Zwecke wären mit dem ursprünglichen Zweck nicht kompatibel: Zum einen steht der Zweck der Erleichterung der Arbeit und der Verbesserung der Arbeitsorganisation nicht im Zusammenhang mit dem Zweck der Überwachung und Beurteilung von Beschäftigten. Der Betroffene muss nicht mit dieser Verarbeitung rechnen. Zum

---

[25] gem. Art. 5 Abs. 1 lit b 2. Halbs. DSGVO gilt für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke die gesetzliche Vermutung der zulässigen Weiterverarbeitung für andere als die ursprünglichen Zwecke

[26] *Monreal*, ZD 2016, 507, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO; a.A. *Schantz*, NJW 2016, 1841, Die DS-GVO – Beginn einer neuen Zeitrechnung im Datenschutzrecht, der hierin einen redaktionellen Fehler sehen will.

anderen aber ist auch die Eingriffsintensität eine völlig andere, so dass eine Rechtfertigung der Datennutzung nicht auf die Zweckänderung gestützt werden kann.

Die begrenzte Zulässigkeit einer Zweckänderung kann auch das integrierte semantische Fabrikgedächtnis nicht rechtfertigen. Jedes Datum, welches in dieser Datenbank gespeichert würde, müsste mit dem konkreten Erhebungszweck versehen werden. Bei Anwendung dieses Datums für einen anderen Zweck müsste dann die Kompatibilitätsprüfung durchgeführt werden. Das steht einer umfassenden Datenbank als Wissensbasis für alle Beschäftigten entgegen. Das integrierte semantische Fabrikgedächtnis zeichnet sich ja gerade dadurch aus, dass die unterschiedlichen Daten, die in einem Unternehmen anfallen, zusammengeführt und ausgewertet werden, ohne dass es bereits eine konkrete Zweckbestimmung gibt. Erst aus den Korrelationen sollen Nutzen und Anwendungsbereiche bestimmt werden. Eine solche Verarbeitung ist somit nur mit anonymisierten Daten zulässig.

1.2.5 Grundsatz der Datenminimierung

Der Grundsatz der Datenminimierung in Art. 5 Abs. 1 lit. c DSGVO besagt, dass Daten im Rahmen der Zweckbindung qualitativ und quantitativ[27] begrenzt werden müssen. Das bedeutet, dass nur solche Daten verarbeitet werden dürfen, die verhältnismäßig[28] zur Erreichung des jeweiligen Zwecks sind. Über die Verhältnismäßigkeit hinaus müssen die Grundsätze der Datenvermeidung und Datensparsamkeit berücksichtigt werden.[29] Auf diesem Grundsatz basieren etwa Art. 25 (Datenschutz *by design and by default*)[30] und das Recht auf Einschränkung der Verarbeitung in Art. 18 DSGVO.

Es bleibt abzuwarten, ob dieser sehr allgemeine Grundsatz Geschäftsmodelle der Industrie 4.0 und der damit einhergehenden Verarbeitung großer Datenmengen verhindert. Vieles spricht dafür, dass aus diesem Grundsatz keine grundsätzliche Unzulässigkeit folgt, dass aber im Einzelfall anhand des Verhältnismäßigkeitsgrundsatzes[31] zu prüfen ist, ob und welche Daten zur Erzielung eines konkreten unternehmerischen Ziels erforderlich sind. Jedenfalls ist zu erwarten, dass nur dann personenbezogene Daten genutzt und gespeichert werden dürfen, wenn eine Anonymisierung dieser Daten zur Erreichung des Zweckes ungeeignet ist. Nur so kann gewährleistet werden, dass der Grundsatz der Datenminimierung auch im Beschäftigtenkontext hinreichend Berücksichtigung findet.

1.2.6 Grundsatz der Datenrichtigkeit

Art. 5 Abs. 1 lit. d DSGVO fordert die Richtigkeit und Aktualität personenbezogener Daten. Dazu sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.[32] Der Grundsatz der Datenrichtigkeit

---

[27] Vgl. EG 39 S. 7-10.
[28] zum europarechtlichen Verhältnismäßigkeitsgrundsatz Vgl. hiernach.
[29] *Heberlein* in: Ehmann/Sehlmayr, DS-GVO, 1. Auflage 2017, Art. 5 Rn. 22.
[30] Vgl. hiernach Gliederungspunkt F.
[31] zum Verhältnismäßigkeitsgrundsatz hiernach D.I.2.
[32] Vgl. auch EG 39 Satz 11.

findet Ausprägungen etwa in Art. 16 und 17 DSGVO (Recht auf Berichtigung und Löschung), aber auch in der Pflicht zur Mitteilung von Berichtigungen an Empfänger nach Art. 19 DSGVO.

1.2.7 Grundsatz der zeitlichen Begrenzung der Speicherung

Der Grundsatz der Speicherbegrenzung entspricht dem Grundsatz der Zweckbindung. Die Speicherung von personenbezogenen Daten ist nur so lange zulässig, wie dies für den jeweils festgelegten Zweck erforderlich ist. Das bedeutet, dass grundsätzlich umgehend nach Erfüllung des Primärzwecks der Personenbezug aufzuheben ist. Das ist beispielsweise durch Anonymisierung der Daten möglich.

Auch dieser Grundsatz spielt für datenbasierte Geschäftsmodelle und Unternehmensprozesse eine wichtige Rolle. Gerade adaptive und selbstlernende Systeme sind darauf angewiesen, aus „alten“ Daten zu lernen, diese mit „neuen“ Daten zu vergleichen und entsprechende Erkenntnisse hieraus abzuleiten. Die zulässige Speicherdauer personenbezogener Daten ist daher in Abwägung mit den Interessen des Arbeitgebers an derartigen adaptiven Systemen und den damit verbundenen Zwecken zu ermitteln.

1.2.8 Datensicherheit als datenschutzrechtlicher Grundsatz der Integrität und Vertraulichkeit

Der in Art. 5 Abs. 1 lit. f DSGVO neu eingeführte Grundsatz der Integrität und Vertraulichkeit fordert, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Der Verantwortliche hat dies durch geeignete technische und organisatorische Maßnahmen umzusetzen.

Bei zunehmend vernetzten Systemen und erheblicher Steigerung der verarbeiteten Daten ergeben sich auch, insbesondere im Beschäftigtenkontext, erhebliche Sicherheits- und Missbrauchsrisiken. Die Einführung adaptiver Assistenzsysteme darf sich daher nicht darauf beschränken, die Verarbeitung der Daten auf eine zulässige Rechtsgrundlage zu stützen. Vielmehr muss das Unternehmen in dem Maße, wie zunehmend personenbezogene Daten verarbeitet werden und die Risiken für diese Daten steigen, entsprechende Sicherheitsvorkehrungen treffen.

1.3 Personenbezogene Daten

Das Datenschutzrecht ist gemäß Art. 1 Abs. 1 DSGVO nur anwendbar, wenn es sich um personenbezogene Daten handelt.

1.3.1 Definition der personenbezogenen Daten

Personenbezogene Daten sind in Art. 4 Nr. 1 DSGVO wie folgt definiert:

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die

Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann."

Beim Einsatz adaptiver Assistenzsysteme fallen häufig Daten an, die zwar einen Bezug zum Beschäftigten haben, nicht aber den Namen oder andere unmittelbare Identifizierungsmerkmale enthalten. Es wird sich daher häufig die Frage stellen, ob bestimmte Daten eine Identifizierung des Beschäftigten ermöglichen oder nicht. Die Beantwortung dieser Frage ist für die rechtliche Bewertung von entscheidender Bedeutung: Von ihr hängt ab, ob die datenschutzrechtlichen Vorgaben Anwendung finden oder nicht.

Eine Identifizierung kann durch ein Autokennzeichen, eine Telefonnummer, die Reisepass- oder Personalausweisnummer, aber auch durch die IP-Adresse[33] erfolgen. Außer aufgrund einer Kennung kann eine Person auch durch besondere Merkmale zur physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität identifizierbar sein.

Um festzustellen, ob eine natürliche Person identifizierbar ist, sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person mit vernünftigem Aufwand wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren[34]. Gemäß Erwägungsgrund 26 ist es für die Qualifikation eines Datenbestandes als personenbezogene Daten nicht notwendig, dass der Verantwortliche selbst die Identifizierung durchführen kann. Vielmehr genügt es, dass irgendein Dritter zur Identifizierung in der Lage ist, wobei Kosten und zeitlicher Aufwand ebenso zu berücksichtigen sind wie die jeweils verfügbare Technologie und die technologische Entwicklung. Durch den ausdrücklichen Bezug auf die technologische Entwicklung dynamisiert die DSGVO den Begriff der Identifizierbarkeit und verpflichtet Verantwortliche, Aufsichtsbehörden und Gerichte, in Zukunft dieser Entwicklung zu folgen und gegebenenfalls die Identifizierbarkeit von Datenbeständen neu zu bewerten.[35] Um den Zweck des Schutzes der betroffenen Personen vor Beeinträchtigung ihrer Grundrechte durch die Verarbeitung von Daten zu erreichen, müssen die tatsächlich verfügbaren und nicht nur die rechtlich zulässigen Möglichkeiten berücksichtigt werden.[36]

Die Pseudonymisierung lässt den Personenbezug, anders als die Anonymisierung, nicht entfallen[37] .

Beim Einsatz adaptiver Assistenzsysteme werden häufig personenbezogene Daten anfallen: Durch das Auslesen von Daten eines Assistenzsystems kann in der Regel bereits aufgrund der Registrierung des Beschäftigten oder durch Verknüpfung mit dem Einsatzplan festgestellt werden, welcher Beschäftigte das Assistenzsystem ge-

---

[33] EuGH BeckRS 2012, 80744 Rn. 51.
[34] *Schild,* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, DSGVO, Art. 4 Rn. 15.
[35] *Brecht/Steinbrück/Wagner*, Der Arbeitnehmer 4.0? PinG 01.18, S. 10, 11.
[36] *Klabunde* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 4 Rn. 13.
[37] Vgl. hierzu näher F.IX.

nutzt hat.[38] Damit erhalten sämtliche vom Assistenzsystem verarbeiteten Daten einen Personenbezug.

1.3.2 Beschäftigtendaten

§ 26 BDSG-neu gilt für die Verarbeitung personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses. Der Beschäftigtenbegriff ist in § 26 Abs. 8 BDSG-neu definiert und umfasst in Anlehnung an den im Wesentlichen inhaltsgleichen § 3 Abs. 11 BDSG-alt neben Arbeitnehmern und Arbeitnehmerinnen unter anderem auch (klarstellend) Leiharbeitnehmerinnen und Leiharbeitnehmer, Berufsauszubildende, Rehabilitandinnen und Rehabilitanden, freie Beschäftigte und Beamte. Auch Bewerberinnen und Bewerber sowie Beschäftigte mit beendetem Arbeitsverhältnis werden über den Beschäftigtenbegriff erfasst,[39] nicht jedoch Organmitglieder, mit denen ein Geschäftsbesorgungsvertrag geschlossen wurde.

1.3.3 Kategorien personenbezogener Daten

1.3.3.1 Nutzerdaten

Viele der adaptiven Arbeitsassistenzsysteme können nur unter Verwendung eines für den Beschäftigten individualisierten Nutzerkontos betrieben werden. Dies ist vor allem bei solchen Systemen der Fall, die den Beschäftigten unter Berücksichtigung seiner individuellen Fähigkeiten unterstützen sollen. Gleichwohl können auch Assistenzsysteme, die die kontextabhängige Aufbereitung und Visualisierung von Informationen zum Gegenstand haben, die Verwendung von individuellen Nutzerkonten erfordern. Bei der auf bestimmte Beschäftigte beschränkten Nutzung für entsprechend berechtigte Beschäftigte muss das Assistenzsystem in der Lage sein, Nutzer zu authentifizieren und autorisieren. Ohne Rückgriff auf Techniken zur Anonymisierung oder Pseudonymisierung kann dies nur mittels Nutzerkonten erfolgen.[40] Diese im Rahmen des Nutzerkontos anfallenden Nutzerdaten sind personenbezogene Daten und unterfallen damit dem Datenschutzrecht.

1.3.3.2 Bilddaten

Für den Einsatz bestimmter kamerabasierter Assistenzsysteme ist die Erfassung von Bilddaten relevant. Dabei werden nur dann personenbezogene Daten erfasst, wenn sich der Personenbezug durch Verknüpfung personenbezogener Daten mit der Aufnahme herstellen lässt. Dazu muss die betroffene Person für den Arbeitgeber erkennbar sein. Können Aufnahmen nicht oder nur mit unverhältnismäßigem Aufwand aus dem Gerät ausgelesen werden, ist allein auf dessen eigene Erkennungsleistung abzustellen. Verfügt das System über keine Fähigkeit zur Bilderkennung, liegen

---

[38] *Brecht/Steinbrück/Wagner*, Der Arbeitnehmer 4.0? PinG 01.18, S. 10, 11.

[39] Dieses weite Verständnis des Arbeitnehmerbegriffs dürfte insoweit auch dem Verständnis des Art. 88 DSGVO entsprechen. Zwar definiert die DSGVO selbst den Beschäftigtenbegriff nicht. Allerdings deckt sich dieses Verständnis mit der Auslegung des europäischen Arbeitnehmer/Beschäftigtenbegriffs, bei der sich der EuGH an dem weiten Begriff der Arbeitnehmerfreizügigkeit in Art. 45 AEUV orientiert. Vgl. EuGH Urt. v. 11.11.2015 – Rs. C-422/14 – Pujante Rivera. So auch *Spelge*, DUD 2016, 776 (777), Der Beschäftigtendatenschutz nach Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO).

[40] Vgl. *Hofmann,* ZD 2016, 12, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0.

schon keine personenbezogenen Daten vor. Ist hingegen die menschliche Betrachtung der Aufnahmen vorgesehen, ist auf die Erkennungsleistung des menschlichen Betrachters abzustellen.[41]

Datenschutzrechtlich relevant ist bereits die Erhebung von personenbezogenen Daten, ohne dass es darauf ankäme, ob sie auch gespeichert werden. Wenn die Aufnahmen zeitgleich ausgelesen und menschlich wahrgenommen werden, spielt es keine Rolle, ob die Aufnahmen auch gespeichert werden. Ist ein Auslesen der Bilddaten hingegen nicht oder nur unter unverhältnismäßigem Aufwand möglich, kommt es darauf an, wie mit den Bilddaten weiter verfahren wird. Werden sie allein gelagert und nach kurzer Verarbeitung wieder gelöscht, besteht keine Erhebung oder Verarbeitung, die datenschutzrechtlich relevant wäre.[42]

1.3.3.3 Videodaten

Kamerabasierte Assistenzsystem, die weder über eine Schnittstelle zum Auslesen der Aufnahmen noch über die Fähigkeit zur automatisierten Personenidentifikation verfügen, unterfallen nicht dem Anwendungsbereich des Datenschutzrechts. Dies können beispielsweise Systeme zur Kollisionsvermeidung sein. Für kamerabasierte Assistenzsysteme die hingegen über eine Schnittstelle zum Auslesen der Aufnahmen verfügen, gelten die allgemeinen Grundsätze zur Videoüberwachung. Die damit erfassten Videobilddaten weisen in der Regel einen Personenbezug auf.[43]

1.3.3.4 Standortdaten

Werden mittels des eingesetzten Assistenzsystems auch Standortdaten erfasst, ist danach zu unterscheiden, ob der Beschäftigte und das Gerät von anderen geortet werden kann oder lediglich das Gerät die selbst ermittelten Positionsdaten an einen anderen übermittelt. Nur im letzteren Fall liegt keine Erhebung personenbezogener Daten vor.[44]

1.3.3.5 Gesundheitsdaten

Je nach Art des adaptiven Arbeitsassistenzsystems werden mittels der Sensorik Daten erhoben, die Rückschlüsse auf die Gesundheit des Beschäftigten zulassen und gerade aus diesem Grund im Arbeitsumfeld eingesetzt werden sollen.

Gesundheitsdaten sind in Art. 4 Nr. 13 DSGVO definiert:

„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienst-

---

[41] Vgl. *Hofmann*, ZD 2016, 12 Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0 m.w.N.

[42] Vgl. *Hofmann* ZD 2016, 12, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0 m.w.N.

[43] Vgl. *Hofmann* ZD 2016, 12, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0 m.w.N.

[44] Vgl. *Hofmann* ZD 2016, 12, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0 m.w.N.

leistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen."

Der Begriff ist somit sehr weit und umfasst auch Informationen, aus denen sich Rückschlüsse auf den Gesundheitszustand einer natürlichen Person schließen lassen. Dies können Vitaldaten, aber auch die Schrittanzahl eines Beschäftigten sein, denn diese lassen Rückschlüsse auf den Gesundheitszustand zu.[45] Gesundheitsdaten gehören zu den besonderen personenbezogenen Daten und unterliegen aufgrund des stärkeren Eingriffs in die Persönlichkeitsrechte des Betroffenen erhöhten Anforderungen. Art. 9 DSGVO sieht ein Verbot der Verarbeitung von Gesundheitsdaten vor, wobei in Abs. 2 eng definierte Ausnahmen geregelt sind. Eine dieser Ausnahmen betrifft das Arbeitsverhältnis und ist in § 26 Abs. 3 BDSG-neu wie folgt umgesetzt:

„abweichend von Art. 9 Abs. 1 DSGVO die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt."

Auch hinsichtlich der Einwilligung eines Beschäftigten in der Verarbeitung besonderer personenbezogener Daten legt § 26 Abs. 3 Satz 2 BDSG-neu erhöhte Anforderungen fest.[46]

1.3.3.6 Biometrische Daten

Zu den besonderen personenbezogenen Daten im Sinne des Art. 9 DSGVO gehören auch biometrische Daten. Biometrische Daten sind in Art. 4 Nr. 14 DSGVO als Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person definiert, die die eindeutige Identifizierung ermöglichen. Biometrische Daten spielen zunehmend bei Zeiterfassungssystemen eine Rolle, können aber auch bei adaptiven Assistenzsystemen Einsatz finden. Gerade im Hochsicherheitsbereich greifen Arbeitgeber häufig auf die Erkennung der Berechtigung eines Beschäftigten auf biometrische Daten zurück.

Aufgrund der nur sehr eingeschränkten Rechtfertigungsmöglichkeit bei der Verarbeitung von biometrischen Daten empfiehlt sich regelmäßig der Weg über eine Kollektivvereinbarung.[47]

---

[45] *Blinn,* DSRITB 2016, 519, Wearables und Arbeitnehmerdatenschutz – Vom freiwilligen Selbstoptimierer zum Kontrollinstrument des Arbeitgebers?

[46] Vgl. hierzu D.IV.

[47] Vgl. hiernach D.III.

2 Rechtsgrundlagen für die Datenverarbeitung bei Anwendung adpativer Assistenzsysteme

Gemäß Art. 6 Abs. 1 DSGVO ist eine Datenverarbeitung nur zulässig, wenn sie auf einer Einwilligung oder auf einem der sonstigen in Art. 6 Abs. 1 lit. b bis f DSGVO genannten Rechtfertigungsgründe beruht.

Als Rechtfertigungsgrund kommt vorliegend vor allem § 26 BDSG-neu in Betracht. Daneben können Art. 6 Abs. 1 lit. f DSGVO, Kollektivvereinbarungen und die Einwilligung zur Anwendung kommen.

2.1 § 26 BDSG-neu als Rechtsgrundlage für die Datenverarbeitung

Der neue § 26 BDSG hat folgenden Wortlaut:

„Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.“

Damit knüpft die neue Regelung an den § 32 BDSG-alt an: Für die Frage der datenschutzrechtlichen Zulässigkeit von adaptiven Assistenzsystemen wird es darauf ankommen, ob die Verarbeitung von personenbezogenen Daten in diesem Zusammenhang für die Durchführung eines Beschäftigungsverhältnisses erforderlich ist.

2.1.1 Anwendungsbereich

§ 26 Abs. 1 Satz 1 BDSG-neu[48] erlaubt die Datenverarbeitung u.a., wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Wie bei jeder Rechtfertigung im Datenschutzrecht, kommt es zunächst darauf an, den konkreten Zweck der Datenverarbeitung zu bestimmen. Die Datenverarbeitung ist nur zulässig, wenn diese zur Erreichung dieses Zwecks erforderlich ist.

Bei der Verarbeitung von Daten im Zusammenhang mit adaptiven Assistenzsystemen geht es regelmäßig nicht oder nicht in erster Linie um das Verhalten oder die betriebliche Situation des einzelnen Beschäftigten, wie z.B. Beschäftigtenbeurteilung, die Leistungskontrolle, die Aufdeckung von Pflichtverletzungen oder Straftaten, Zugangskontrollen, Arbeitsschutz oder die Personalverwaltung. Bei der Datenverarbeitung zu diesen Zwecken steht der Beschäftigte im Mittelpunkt. Die personenbezogenen Daten werden verarbeitet, um die Arbeit des betroffenen Beschäftigten zu organisieren, zu gestalten und zu kontrollieren. Die Bankverbindung des Beschäftigten

[48] Entsprechend nach der bisherigen Rechtslage § 32 BDSG-alt.

wird benötigt, um sein Gehalt zu überweisen. Körpermaße werden abgefragt, um dem Beschäftigten einen ergonomischen Arbeitsplatz einzurichten und seine Kenntnisse und Erfahrungen dienen dem Zweck, eine für den Beschäftigten passende Aufgabe zu finden. Dieser Datenverarbeitungszweck steht im Mittelpunkt der bisherigen Diskussion in der juristischen Literatur und Rechtsprechung.

Bei adaptiven Assistenzsystemen geht es demgegenüber um die Betriebsorganisation und -steuerung. Die Optimierung von betrieblichen Prozessen, die organisatorische Umgestaltung von Arbeitsabläufen sowie die Entwicklung neuer Geschäftsmodelle stehen im Vordergrund. [49] Das Leitbild der Industrie 4.0-Anwendungen besteht in der umfassend vernetzten Fabrik. Es geht um die digitalen Organisation und Steuerung des Wertschöpfungsvorgangs, der sich auf den gesamten Lebenszyklus von Erzeugnissen erstreckt und vertikal von der Produktentwicklung über Produktion und Logistik bis hin zum Vertrieb und Service sowie horizontal über die Unternehmensgrenzen hinweg von Zulieferern und Dienstleitern über das Herstellungsunternehmen bis hin zum Endkunden und zum Recycling reicht.[50] Viele dieser Daten werden anonymisierte oder von vorneherein nicht personenbezogene Daten sein. Dennoch werden auch Beschäftigtendaten in diesem Zusammenhang in großem Umfang verarbeitet werden.

Soll den Beschäftigte anhand adaptiver Assistenzsysteme Handlungs- und Prozesswissen vermittelt werden oder sind der Arbeitsschutz, die Arbeitserleichterung und Fortbildung der Beschäftigten Teil der mit den Assistenzsystemen gestalteten Arbeitsorganisation, so ist der Bezug zum Beschäftigungsverhältnis evident. Geht es aber in erster Linie um die Steuerung und Organisation des Unternehmens, um die Steigerung der Effektivität technischer oder logistischer Abläufe, fehlt es ggf. an einem solchen unmittelbaren Bezug.[51] Es ist daher zu klären, ob die digitale Gestaltung des Beschäftigtenumfeldes noch einem Zweck dient, der zur Durchführung des Beschäftigtenverhältnisses erforderlich ist.

Was unter „Zwecke des Beschäftigungsverhältnisses“ im Sinne des § 32 BDSG-alt zu verstehen ist, ist in der Literatur umstritten und ist auch durch § 26 Abs. 1 Satz 1 BDSG-neu nicht geklärt. Nach einem engen Verständnis sollen darunter nur solche Zwecke fallen, die der Erfüllung der gegenseitigen Hauptleistungspflichten des Arbeitgebers und des Beschäftigten dienen.[52] Ein sehr weiter Ansatz will unter Zwecke des Beschäftigungsverhältnisses alle Zwecke fassen, die mit dem Arbeitsverhältnis in einem ursächlichen Zusammenhang stehen, somit nicht ausschließlich Zwecke des arbeitsvertraglich vereinbarten Leistungsaustausches. Dazu gehören nach dieser Ansicht nicht nur die Hauptpflichten, sondern jede mit dem Beschäftigungsverhältnis in Zusammenhang stehende Wahrnehmung von Rechten.[53] Danach würden dann auch arbeitsvertragliche Nebenpflichten, wie die Duldung von Kontrollen oder

---

[49] Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 7.

[50] *Krause*, Expertenbericht Digitalisierung und Beschäftigtendatenschutz, Bundesministerium für Arbeit und Soziales, November 2016, S. 14.

[51] Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 7.

[52] *Joussen*, NZA 2010, 254 (258), Die Zulässigkeit von vorbeugenden Torkontrollen nach dem neuen BDSG.

[53] *Schmidt* DuD 2010, 207 (209), Beschäftigtendatenschutz in § 32 BDSG; *Wybitul*, Datenschutz im Unternehmen, 2011, Anh. 3, S. 428.

Maßnahmen zur Verhinderung von Straftaten unter § 32 BDSG-alt fallen.[54] Erst wenn der Arbeitgeber den Beschäftigten wie ein beliebiger Dritter gegenübersteht, soll § 32 BDSG-alt nicht mehr greifen.[55]

Durchgesetzt hat sich in der Literatur zum BDSG-alt eine vermittelnde Ansicht. So können auch Datenverarbeitungsvorgänge, die nicht der Erfüllung einer arbeitsvertraglichen Hauptpflicht dienen, durch § 32 BDSG-alt gedeckt sein. Die Datenverarbeitung muss aber im Zusammenhang mit der Tätigkeit des Beschäftigten stehen und darf nicht allein anlässlich einer Maßnahme zur Arbeitsorganisation anfallen. Die Digitalisierung des Arbeitsplatzes ist eine Maßnahme im Interesse des Unternehmers, die nur dann von § 32 BDSG-alt gedeckt ist, wenn ein konkreter Bezug zum Arbeitsverhältnis des Beschäftigten besteht.

Die Nachfolgeregelung in § 26 BDSG-neu wurde unter der Öffnungsklausel des Art. 88 DSGVO erlassen. Der Anwendungsbereich des § 26 BDSG-neu ist somit durch diese Vorschrift begrenzt. Es ist also zu fragen, ob Art. 88 Abs. 1 DSGVO dem nationalen Gesetzgeber ermöglicht, über den engen Beschäftigungskontext hinaus nationale Regelungen zu erlassen, die auch die digitale Gestaltung des Unternehmens in Gänze umfassen. Dies ist zu bejahen:

Nach dem Wortlaut von Art. 88 DSGVO dürfen die nationalen Gesetzgeber nicht nur Regelungen bezüglich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext zur Erfüllung des Arbeitsvertrags erlassen, sondern können diese Regelungen u.a. auch Zwecke des Managements, der Planung und der Organisation der Arbeit sowie des Schutzes des Eigentums der Arbeitgeber und der Kunden umfassen. Die Öffnungsklausel erlaubt damit dem nationalen Gesetzgeber spezifischere Regelungen nicht nur bei der Verarbeitung von Beschäftigtendaten zur Durchführung des Arbeitsvertrags, sondern darüber hinaus insbesondere auch zu Managementzwecken und zur Arbeitsorganisation.

Daran schließt sich die Frage an, ob der deutsche Gesetzgeber mit § 26 BDSG-neu von diesem weiten Regelungsermessen auch Gebrauch gemacht hat. Tatsächlich fällt hier auf, dass § 26 Abs. 1 BDSG-neu als Beschäftigungszweck lediglich die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses nennt. Management oder Arbeitsorganisation werden nicht erwähnt. Der in Art. 88 Abs. 1 DSGVO erwähnte Schutz des Eigentums wird in Satz 2 unter den Regelungen zur Aufdeckung einer Straftat gesondert geregelt. Auch aus der Gesetzesbegründung wird deutlich, dass der Gesetzgeber lediglich den Umfang des § 32 BDSG-alt fortführen wollte, aber keine inhaltliche Erweiterung bezweckt hat. So heißt es in der Gesetzesbegründung[56]:

„Der Gesetzgeber behält sich vor, Fragen des Datenschutzes im Beschäftigungsverhältnis innerhalb dieser Vorschrift oder im Rahmen eines gesonderten Gesetzes konkretisierend bestimmte Grundsätze, die im Rahmen der Rechtsprechung zum

---

[54] *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, § 32 Rn. 28.

[55] *Taeger/Rose*, BB 2016, 819 (823), Zum Stand des deutschen und europäischen Beschäftigtendatenschutzes.

[56] BT-Dr 18/11325, S. 97.

geltenden Recht bereits angelegt sind, zu regeln. Dies gilt insbesondere für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken."

Hieraus wird deutlich, dass der Gesetzgeber bewusst keine gegenüber § 32 BDSG-alt erweiterte Rechtsgrundlage schaffen wollte, somit insbesondere auch neue Fragestellungen, die sich durch die digitale Organisation des Arbeitsumfeldes ergeben können, einer gesonderten Regelung vorbehalten wollte.

Im Ergebnis ist somit festzuhalten, dass zwar Art. 88 Abs. 1 DSGVO dem nationalen Gesetzgeber die Möglichkeit eingeräumt hat, auch die Verarbeitung von Beschäftigtendaten zu Zwecken der digitalen Arbeitsorganisation und -planung zu regeln, dass jedoch der deutsche Gesetzgeber von dieser Befugnis lediglich in dem Umfang Gebrauch gemacht hat, als die Datenverarbeitung im unmittelbaren Zusammenhang mit der Erfüllung arbeitsvertraglicher Pflichten steht.

Daraus folgt, dass § 26 BDSG-neu für die Datenverarbeitung im Zusammenhang mit adaptiven Assistenzsystemen nur dann eine Rechtsgrundlage bietet, wenn diese Verarbeitung im Zusammenhang mit der konkreten Erfüllung der Pflichten aus dem Arbeitsvertrag steht. Dies ist in folgenden Fällen anzunehmen:

- Die Datenverarbeitung dient der Erleichterung oder Verbesserung der Tätigkeit des Beschäftigten. Hierzu zählen Assistenzsysteme, wie beispielsweise Anweisungen per Datenbrille, Wearables oder intelligenter Handschuhe[57], die Lokalisation des Fahrers zur Steuerung der Fahrten, Handscanner, die von Pickern genutzt werden[58] und die Erfassung von Beschäftigtendaten im Rahmen einer Mensch-Maschine-Interaktion.[59]
- Die Datenverarbeitung dient zur Kontrolle des Beschäftigten, um ggf. neue Weisungen auszugeben. Hierunter fällt bspw. die Nutzung von RFID-Technik zur Zeiterfassung, zur Zutrittskontrolle oder zur Kontrolle eines Wachmanns bei seinem Rundgang oder einer Routineuntersuchung eines Wartungstechnikers.[60]
- Die Datenverarbeitung dient zur Verbesserung der Arbeitssicherheit und des Gesundheitsschutzes, wie z.B. die Ortung eines Beschäftigten zum Schutz seiner persönlichen Sicherheit.[61]
- Die Datenverarbeitung dient der Effektivierung der betrieblichen Abläufe. Dabei muss jedoch die konkret bezweckte Verbesserung bei Datenerhebung feststehen und darf nicht erst anhand der Daten ermittelt werden. Zu bejahen ist ein solcher

[57] Beispiel aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 15.
[58] Beispiel aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 16.
[59] Beispiel aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 15.
[60] Beispiele aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 10.
[61] Beispiel aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 26.

Zweck bei der Ortung von Fahrzeugen zur verbesserten Einsatzplanung der Fahrzeuge.[62]

Werden demgegenüber Daten verarbeitet, die nur allgemein der Arbeitsorganisation und -planung dienen, kommt § 26 BDSG-neu nicht in Betracht. Hierzu gehören folgende Fallgestaltungen:

- Daten werden zunächst ohne konkreten Zweck erfasst. Erst aus der Verarbeitung einer großen Anzahl von Daten sollen Rückschlüsse auf Arbeitsweisen und Organisationsverbesserungen gezogen werden.
- Die Ortung eines Beschäftigten, bspw. eines Geldtransporters dient dem Schutz von Arbeitgebereigentum oder Kunden.[63]
- Beschäftigtendaten werden während der Arbeitsausführung erhoben und anhand dieser Daten werden individuelle Nutzerkonten erstellt, um anschließend Rückschlüsse auf Fähigkeiten und Einsatzmöglichkeiten zu ziehen.[64]

Die Übersicht zeigt, dass der Einsatz von adaptiven Assistenzsystemen in den meisten Konstellationen in den Anwendungsbereich von § 26 BDSG-neu fällt. Steht der Verarbeitungszweck jedoch nicht im Beschäftigtenkontext, wie beispielsweise beim Schutz des Kundeneigentums oder die Erstellung eines semantischen Fabrikgedächtnisses ist § 26 BDSG-neu nicht anwendbar. Auch wenn Daten erhoben werden, deren Zweck noch nicht konkret feststeht, sondern deren Nutzen erst aus der Verarbeitung einer Vielzahl von Daten ermittelt werden soll, kommt § 26 BDSG-neu nicht als Rechtfertigung in Betracht.

In diesen Fällen ist zu prüfen, ob der Einsatz von adaptiven Assistenzsystemen auf die Interessenabwägung nach Art. 6 Abs. 1 f DSGVO gestützt werden kann.[65]

2.1.2 Die Voraussetzungen im Einzelnen

2.1.2.1 Erforderlichkeit

2.1.2.1.1 Die Erforderlichkeit nach § 32 BDSG-alt

Bis zur Einführung des § 32 BDSG-alt zum 14. September 2009 war die Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten § 28 BDSG-alt. Die Verarbeitung von Daten eines Beschäftigten galt damit als eine Fallgruppe der Datenverarbeitung im Rahmen der Vertragserfüllung. Eine spezielle Beschäftigtenregelung enthielt erstmals § 32 BDSG-alt. Die Regelung war zunächst nur als Provisorium gedacht

---

[62] in diesem Sinn: *Krause*, Expertenbericht Digitalisierung und Beschäftigtendatenschutz, Bundesministerium für Arbeit und Soziales, S. 27.

[63] Beispiel aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 26. Auch *Krause* hält § 32 BDSG-alt in diesem Fall für nicht anwendbar.

[64] Beispiel aus Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 15.

[65] Vgl. hiernach B.III.

und sollte gegenüber der vorherigen Rechtslage wenige Änderungen bringen.[66] Nach der damaligen Gesetzesbegründung sollte die Regelung durch ein umfassenderes Arbeitnehmerdatenschutzgesetz ersetzt werden.[67]

Das zentrale Element des § 28 Abs. 1 S.1 BDSG-alt[68] bestand in einer klassischen Verhältnismäßigkeitsprüfung, mit der die informationelle Selbstbestimmung des Beschäftigten und die ebenfalls grundrechtlich geschützten unternehmerischen Freiheits- und Eigentumsrechte des Arbeitgebers in Ausgleich gebracht werden sollten. So hatte das Bundesarbeitsgericht (BAG)[69] darüber zu entscheiden, ob ein Bewerber die Vernichtung eines Fragebogens mit zahlreichen persönlichen Angaben verlangen durfte, nachdem seine Bewerbung abgelehnt worden war. Das BAG führte hierzu aus, dass eine Verletzung des Persönlichkeitsrechts des abgelehnten Bewerbers dann nicht vorläge, wenn ein berechtigtes Interesse des Arbeitgebers an der Aufbewahrung des Fragebogens bestünde. Ein solches Interesse sah das BAG allerdings nicht in der Absicht, den Fragebogen im Falle einer erneuten Bewerbung zu einem Datenabgleich heranzuziehen. Das BAG begründete dies damit, dass das Mittel der Aufbewahrung des Fragebogens zum einen nicht geeignet sei, diesen Zweck zu erreichen, da sich die Daten verändern können. Zudem hielt das BAG die Aufbewahrung für nicht erforderlich. Der Arbeitgeber möge zwar, so das BAG, ein berechtigtes Interesse daran haben, sich die Namen der erfolglosen Bewerber festzuhalten, um im Falle einer nochmaligen Bewerbung evtl. Verwaltungs- und Vorstellungskosten einzusparen. Dafür reiche es jedoch aus, wenn die Person des Bewerbers ausreichend charakterisierenden persönliche Daten wie Name, Anschrift und Geburtsdatum gespeichert werden. Die Aufbewahrung des Einstellungsfragebogens mit den viel weitergehenden Auskünften übersteige dagegen dieses Informationsbedürfnis.

Diese zu § 28 Abs. 1 S.1 BDSG-alt entwickelten Grundsätze haben auch im Anwendungsbereich des § 32 Abs. 1 BDSG-alt weiter Bestand: Obwohl § 32 Abs. 1 BDSG-alt nur die Erforderlichkeit erwähnt, soll nach Literatur Rechtsprechung weiterhin das ungeschriebene Erfordernis der Verhältnismäßigkeit gelten.[70]

Die klassische Verhältnismäßigkeitsprüfung enthält drei Prüfungsschritte[71]:

- Die Maßnahme muss zur Erreichung des (legitimen) Zwecks geeignet sein, d.h. muss zur Erreichung des Zwecks förderlich sein.

---

[66] *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition Stand: 01.08.2017, § 32 Rn.; *Franzen* in: Müller-Glöge/Preis/Schmidt, Erfurter Kommentar zum Arbeitsrecht, 17. Aufl. 2017, § 32 BDSG Rn. 6-7; ob die Einführung des Erforderlichkeitskriteriums Änderungen bewirkten, wird eingehend diskutiert bei *Thüsing*, NZA 2009, 865, Datenschutz im Arbeitsverhältnis – Kritische Gedanken zu § 32 BDSG.

[67] BT-Drs. 16/13657, 20.

[68] der früher noch auf die „Dienlichkeit" abstellte, von Literatur und Rspr. jedoch ebenfalls im Sinne einer Verhältnismäßigkeitsprüfung verstanden wurde.

[69] BAG Urt. v. 6.6.1984 – 5 AZR 286/81 in NZA 1984, 321.

[70] BAGE 146, 109 in NZA 2014, 41; *Stamer/Kuhnke* in: Plath, BDSG, § 32 Rn. 17f.; *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, § 32 BDSG.

[71] *Klatt/Meister*, JuS 2014, 193, Der Grundsatz der Verhältnismäßigkeit; BAG, Beschluss v. 29.6.2004 – 1ABR 21/03 in: NJW 2005, 313.

- Die Maßnahme muss zur Erreichung des Zwecks erforderlich sein. Die Erforderlichkeit ist gegeben, wenn es kein anderes, gleich geeignetes Mittel gibt, das weniger intensiv in das Grundrecht des Betroffenen eingreift.
- Die Verhältnismäßigkeitsprüfung (im engeren Sinne) erfolgt durch Bestimmung des Grads der Eingriffsintensität und die Wichtigkeit des verfolgten Zwecks, wobei untersucht wird, ob die Wichtigkeit des verfolgten Ziels die Intensität des Eingriffs rechtfertigen kann.

Unklar war bei Einführung des § 32 BDSG-alt allerdings, ob die Einführung der Erforderlichkeitsprüfung nicht nur eine Interessenabwägung, sondern zusätzlich auch eine Prüfung der Alternativlosigkeit der Datenerhebung notwendig machen würde. Mehrheitlich wurde eine solche Verschärfung allerdings abgelehnt und das Merkmal der Erforderlichkeit weiterhin als Erfordernis einer Interessenabwägung verstanden, wie sie bereits unter § 28 BDSG durchzuführen war.[72]

Im Rahmen des § 32 BDSG-alt wird das Merkmal der Erforderlichkeit nach diesem Verständnis nicht im Sinne einer Pflicht zur Verwendung des aus Sicht des Beschäftigten am wenigsten einschneidenden Mittels ausgelegt, weil dem Arbeitgeber im Rahmen seiner Unternehmerfreiheit ein Entscheidungsspielraum über die Organisation betrieblicher Abläufe zukommt.[73] Erforderlichkeit ist daher nicht im Sinne einer objektiven Unverzichtbarkeit oder Alternativlosigkeit zu verstehen, die von den Gerichten uneingeschränkt überprüfbar wäre. Vielmehr ist auch die Frage der Erforderlichkeit i.S.d. § 32 BGSG-alt durch eine Interessenabwägung zu ermitteln. Dabei bleibt dem Arbeitgeber ein gewisser Spielraum, selbst zu entscheiden, welche Verfahren zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten eingesetzt werden.[74]

2.1.2.1.2 Die Erforderlichkeit nach § 26 BDSG-neu

Auch § 26 BDSG-neu sieht vor, dass die Datenverarbeitung für die genannten Zwecke erforderlich sein muss. Die Übernahme des Kriteriums der Erforderlichkeit in den § 26 Abs. 1 Satz 1 BGSG-neu ist auf Kritik gestoßen. Das Erforderlichkeitskriterium sei bereits unter § 32 BGSG-alt nicht wörtlich zu nehmen. Es gäbe nämlich kaum personenbezogene Daten, deren Erhebung und Verarbeitung für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich im Sinne zwingender Notwendigkeit seien. Vielmehr gehe es bei der Erforderlichkeit um eine Anwendung des Verhältnismäßigkeitsprinzips und damit implizit um eine Abwägung der Interessen des datenerhebenden und datenverarbeitenden Arbeitgebers mit den Interessen des betroffenen Beschäftigten. Der Gesetzgeber hätte besser das Verhältnismäßigkeitsprinzip und die Interessenabwägung im Gesetzestext aufnehmen sollen.[75]

---

[72] in diesem Sinne auch *Gola/Klug/Körffer* in: Gola/Schomerus, BDSG, 12. Auflage 2015, § 32 Rn. 9; *Däubler*, NZA 2001, 874, Das Neue Bundesddatenschutzgesetz und seine Auswirkungen im Arbeitsrecht.

[73] *Gola/Klug/Körffer* in: Gola/Schomerus, BDSG, 12. Auflage 2015, § 32 Rn.10.

[74] *Erfurth*, NJOZ 2009, 2914, Der „neue“ Arbeitnehmerdatenschutz im BDSG; BAG *Beschluss* v. 29.06.2004 – 1 ABR 21/03 (LAG Berlin) in: NJW 2005, 313.

[75] *Kort* ZD 2017, 319 (320), Der Beschäftigtendatenschutz gem. § 26 BDSG-neu.

Tatsächlich geht es bei der Anwendung des § 26 BDSG-neu, wie bereits unter § 32 BDSG-alt, darum, widerstreitende Interessen zum Ausgleich zu bringen.[76] Der Beschäftigte kann sich auf das Recht zur informationellen Selbstbestimmung und dem Schutz seiner Persönlichkeit berufen, um sich gegen die Datennutzung zu wehren.[77] Demgegenüber stehen die ebenfalls grundrechtlich geschützten Positionen des Arbeitgebers: das Eigentumsrecht aus Art. 14 GG, die unternehmerische Freiheit aus Art. 12 GG sowie die Vertragsfreiheit aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG. Der Unternehmer ist daher grundsätzlich berechtigt, Unternehmensziele und Unternehmensorganisation zu bestimmen, ungeachtet der Tatsache, dass die Umsetzung auch Auswirkungen auf das Ausmaß benötigter Daten haben mag. Erst wenn im Rahmen der Abwägung dem Schutz der persönlichen Daten des Beschäftigten Vorrang einzuräumen ist, muss der Unternehmer eine Begrenzung dieser unternehmerischen Freiheiten hinnehmen.

2.1.2.1.3 Anwendungsfälle

In der Literatur wird allgemein vertreten, dass Beschäftigtendaten nicht zur Überwachung oder personenbezogenen Profilbildung und -analyse genutzt werden dürfen. Es sei grundsätzlich unzulässig, mithilfe der kombinierten Nutzung verschiedener Kontrollinstrumente oder anlassloser Dauerüberwachung Bewegungsprofile der Beschäftigten zu erstellen oder ihre sozialen Interaktionen zu kartieren und dabei gar in ihre Intimsphäre einzudringen.[78]

Tatsächlich ist jedoch im Einzelfall zu prüfen, ob die Datenverarbeitung zur Erfüllung des Arbeitsvertrages erforderlich ist. So ist beispielsweise anerkannt, dass im Hochsicherheitsbereich derartige Bewegungsprofile zulässig sind. Die Datenverarbeitung erfolgt in solchen Konstellationen auch zum Schutze des Beschäftigten. Zwar stellt die Erstellung eines Bewegungsprofils einen Eingriff in das Persönlichkeitsrecht des Beschäftigten dar. Dieser Eingriff ist jedoch weniger stark, wenn er auch im Eigeninteresse des Beschäftigten erfolgt, nämlich dem Interesse, vor Schäden bewahrt zu werden. Das Persönlichkeitsrecht muss daher hinter dem Interesse des Arbeitgebers, jederzeit die Sicherheit seiner Beschäftigten zu gewährleisten, zurückstehen. Allerdings ist bei derartigen Maßnahmen immer auch zu prüfen, ob nicht eine datenschutzfreundlichere Variante zur Verfügung steht, die dem Arbeitgeber zumutbar ist.

Die Frage der Verhältnismäßigkeit der Datenverarbeitung lässt sich gut anhand des Beispiels von Kopp/Sokoll[79] illustrieren:

Ein Unternehmen hat die herkömmlichen ID-Zugangskarten für Beschäftigte und Besucher am Betriebseingang durch eine Zugangsmanagement-Anwendung ersetzt, die mit einer Besuchermanagement-App und einem Identifizierungsarmband arbeitet. Dieses verifiziert die Identität über das eindeutige Merkmal des persönlichen Herzrhythmus. Gewiss ist dies eine zuverlässige, unaufwändige Art der Identifizierung. Gleichwohl darf im Geltungsbereich des BDSG stark bezweifelt werden, ob regelmä-

---

[76] *Brecht/Steinbrück/Wagner*, Der Arbeitnehmer 4.0? PinG 01.18, S. 10, 11.
[77] *Riesenhuber* in: BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, § 32 Rn. BDSG 44; BVerfG in MMR 2007, 93 (94).
[78] *Kopp/Sokoll*, a.a.O. S. 1355.
[79] *Kopp/Sokol*l, a.a.O. S. 1355

ßige Aufzeichnungen über den Herzrhythmus eines Beschäftigten, die auch über seinen Gesundheitszustand Aufschluss geben könnten, nur aus dieser Effizienzerwägung heraus erhoben und gespeichert werden dürfen.

Problematisch ist auch der Einsatz von Wearables zum Zweck, das Arbeitsverhalten der Beschäftigte aufzuzeichnen und automatisch zu bewerten. So gibt es eine auch als Finger-Sensor vorstellbare „Team-App“ für Freelancer auf Crowdworking-Plattformen, die Tastenanschläge und Mausbewegungen am Computer überwacht und regelmäßig Screenshots des Computerbildschirms an den Auftraggeber sendet. Sie wird zur Ermittlung des exakten Tätigkeitsumfangs und der danach berechneten Vergütung eingesetzt. Die permanente Überwachung der Leistung eines Beschäftigten dürfte in diesem Fall nicht verhältnismäßig sein, selbst wenn sich die Höhe der Vergütung aus der Anzahl eingetippter Wörter oder dem Umfang von Recherchetätigkeiten ergibt. Auch das dauerhafte Mithören von Telefongesprächen zur Qualitätssicherung in Call-Centern wird als unzulässig angesehen, weil es nicht mehr verhältnismäßig ist. Die Maßnahme muss vielmehr konkret der Beschäftigtenschulung oder Stichprobenkontrolle dienen, den Beschäftigten vorab bekannt gemacht werden, zeitlich begrenzt sein und darf nur in längeren Abständen wiederholt werden.[80]

Aus Schweden wird berichtet, dass sich Beschäftigte RFID-Funkchips implantieren lassen, die Zugangs- und Kundenkarten ersetzen oder die Bedienung von Kopierern erleichtern.[81] Auch derartige Maßnahmen wären unverhältnismäßig: Der Zweck der Zugangs- oder Kopierkontrolle kann durch wesentlich weniger belastende Maßnahmen erfolgen.

Dagegen sind nachfolgende Anwendungen regelmäßig verhältnismäßig:

- Sensoren in der Schutzkleidung von Rettungskräften oder von Arbeitskräften, die mit gefährlichen Stoffen arbeiten, dienen dem überragenden Zweck höherer Betriebssicherheit, also auch zum Schutz von Leib und Leben der Beschäftigten. Es spricht datenschutzrechtlich nichts dagegen, dass sie die hierfür nötigen Informationen zu Arbeitseinsätzen und -umständen aufzeichnen. Sie werden, ähnlich wie bereits eingesetzte Smartphone-Apps zur GPS-Ortung z.B. von Sicherheitskräften in Notfällen, grundsätzlich zulässig sein. Wie in anderen Fällen der betrieblichen IT-Nutzung kommt es darauf an, gemäß den Geboten der Zweckbindung und Erforderlichkeit, klare Regeln festzulegen, wofür und wie diese Technik eingesetzt wird.
- Tragbare Zeitmessgeräte für Schichtarbeiter können ihnen Informationen zu eigenen Schichten liefern und spontane Abstimmungen untereinander ermöglichen, aber auch Angaben über Einsätze von Kollegen in neuem Umfang abrufbar machen. Ähnlich wie bei entsprechenden Funktionalitäten auf dem Diensthandy dürfte bei entsprechend datenschutzkonformer Ausgestaltung solcher Datenuhren (z.B. ohne Verwendung von „Profilen“ über An- und Abwesenheiten anderer Kollegen) eine Anwendung verhältnismäßig sein.

---

[80] *Kopp/Sokoll*, a.a.O. S. 1358.

[81] http://www.spiegel.de/karriere/schweden-cyborg-firma-implantiert-mitarbeitern-mikrochips-a-1141826.html; vgl. auch: https://www.welt.de/wirtschaft/webwelt/article147126453/Darum-habe-ich-mir-einen-Chip-unter-die-Haut-gespritzt.html.

- Auch Wearables zur Optimierung von Betriebsabläufen, wie das mit einer Datenbrille „herumtragbare“ Instandhaltungsbuch in der Werkstatt oder eine Lagerwege weisende und Pakete scannende Logistikbrille, dürften grundsätzlich zulässig sein. Allerdings muss sichergestellt sein, dass die personenbezogenen Daten des Beschäftigten ausschließlich für diesen konkreten Zweck verarbeitet werden.

Grundsätzlich kann festgestellt werden, dass alle Maßnahmen, die zu einer Dauerüberwachung der Beschäftigten[82] oder zu einer vollständigen Profilbildung führen, bspw. weil Daten verschiedener Erfassungssysteme zusammengeführt werden, nicht zulässig sind.[83]

2.1.2.2 Zweckbindung

Das Verbot, Daten auf Vorrat für einen nicht bestimmten Zweck zu erheben und zu speichern, ist ein wesentlicher datenschutzrechtlicher Grundsatz, sowohl nach nationalem Recht, als auch unter der DSGVO.[84] Grundsätzlich ist der Zweck der Verarbeitung auch vor Verarbeitung, also insb. vor Datenerhebung konkret zu bestimmen.

Allerdings wurde dieser Grundsatz im Anwendungsbereich von § 32 BDSG-alt nicht strikt eingehalten und zunehmend aufgeweicht:

Bereits das BAG hat entschieden, dass der Arbeitgeber neben den Daten über die Person des Beschäftigten auch solche über dessen Qualifikation und Einsatzfähigkeit speichern und nutzen dürfe. Es dürfen alle Stammdaten gespeichert werden, die für den zukünftigen Verlauf des Arbeitsverhältnisses von Bedeutung werden können. Dabei stellt das BAG zur Berechtigung nur möglicherweise zukünftig benötigter Personaldaten unter Hinweis auf die Wirtschaftlichkeit des EDV-Einsatzes fest, dass die Zweckbestimmung des Arbeitsverhältnisses auch ggf. die Speicherung solcher Daten in einem Personalinformationssystem rechtfertige, deren Kenntnis erst im Verlauf des Arbeitsverhältnisses erforderlich werden könne.[85] Auch Regelbeurteilungen sind ohne konkreten Entscheidungsbedarf zulässig.[86]

Die DSGVO hat den Grundsatz der Zweckbindung weiter aufgeweicht und ermöglicht die Datenverarbeitung für andere Zwecke, wenn eine Vereinbarkeit zu dem ursprünglichen Erhebungszweck besteht.[87]

Vor diesem Hintergrund ist auch eine flexiblere Anwendung des Zweckbindungsgrundsatzes beim Einsatz von adaptiven Assistenzsystemen im Beschäftigtenkontext zu erwarten. Adaptive Assistenzsysteme sind bereits begriffsmäßig darauf ausgelegt, anhand der erhobenen Daten dazuzulernen. Dies schließt eine Verarbeitung der Daten zu weiteren ursprünglich nicht vorgesehenen Zwecken ein. Die DSGVO ermöglicht die Datenverarbeitung auch für neue Zwecke, solange sie von der Zielrichtung

---

[82] *Brecht/Steinbrück/Wagner*, Der Arbeitnehmer 4.0? PinG 01.18, S. 10,12
[83] BAG, Beschl. v. 27.5.1986 – 1 ABR 48/84, NZA 1986, 643; *Gola* in: Gola, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 102.
[84] Vgl. hierzu bereits C.II.4
[85] *Gola* in Gola, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 95-114, unter Verweis auf Urt. v. 22.10.1986 – 5 AZR 660/85, DB 1987, 1048 am Bsp. des Merkmals „Familienstand“.
[86] Urt. v. 18.11.2008 – 9 AZR 865/07, NJW 2009, 1627.
[87] *Brecht/Steinbrück/Wagner*, Der Arbeitnehmer 4.0? PinG 01.18, S. 10, 13.

und Eingriffsintensität vergleichbar sind. Diese Voraussetzungen werden im Regelfall erfüllt sein. Die Grenze wird erreicht, wenn ein „semantisches Fabrikgedächtnis“ zweckungebunden Daten sammelt und dann für unterschiedlichste Zwecke auswertet und nutzt.

2.2 Berechtigte Interessen des Arbeitgebers gemäß Art. 6 Abs. 1 lit. f DSGVO

Nach Art. 6 Abs. 1 lit. f DSGVO ist die Verarbeitung personenbezogener Daten auch dann rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des für die Verarbeitung Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte der betroffenen Person überwiegen. Hierbei handelt es sich um die zentrale Abwägungsklausel der DSGVO.[88]

Allerdings stellt sich die Frage, ob dieser Erlaubnistatbestand auch bei Beschäftigtendaten greift oder ob § 26 BDSG-neu eine abschließende Spezialregelung enthält. Darüber hinaus ist zu klären, ob und wenn ja welche Unterschiede zu § 26 BDSG-neu bestehen oder ob es nicht in beiden Fällen auf eine Verhältnismäßigkeitsprüfung hinausläuft, in deren Rahmen die widerstreitenden Interessen gegeneinander abzuwägen sind.

Bei der Frage nach der praktischen Relevanz dieser Verarbeitungsbefugnis ist zu berücksichtigen, dass dem Betroffenen ein Widerspruchsrecht nach Art. 21 Abs. 1 DSGVO zusteht.[89]

2.2.1 Abgrenzung zu § 26 BDSG-neu

Die DSGVO findet Anwendung, soweit nicht spezifische Reglungen zum Beschäftigtendatenschutz erlassen wurden oder soweit kein „Beschäftigtenkontext“ vorliegt.[90] Haben Mitgliedstaaten somit nicht oder nur unvollständig von der Öffnungsklausel in Art. 88 DSGVO Gebrauch gemacht, finden die allgemeinen Bestimmungen, insb. Art. 6 DSGVO Anwendung.[91] Auch soweit der Anwendungsbereich des Art. 88 DSGVO nicht eröffnet ist, ist Art. 6 DSGVO Rechtfertigungsgrundlage für die Datenverarbeitung.[92] Art. 88 DSGVO selbst enthält keine materiell-rechtlichen Regelungen zur Verarbeitung von Beschäftigtendaten.[93]

Wie oben festgestellt[94], hat der deutsche Gesetzgeber nur begrenzt von der Öffnungsklausel in Art. 88 DSGVO Gebrauch gemacht. Daher geht § 26 BDSG-neu als speziellere Regelung dem Art. 6 DSGVO nur insoweit vor, als Beschäftigtendaten für Zwecke des Beschäftigtenverhältnisses verarbeitet werden und insb. die Verarbeitung zur Erfüllung des Arbeitsvertrags erforderlich ist. Erfolgt demgegenüber die Ver-

---

[88] *Schulz,* in: Gola, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 50.
[89] Vgl. hiernach Ziff. II.4.
[90] *Imping*, CR 2017, 378 (379), Neue Zeitrechnung im (Beschäftigten-)Datenschutz.
[91] *Selk* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 88, Rn. 9.
[92] *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition Stand 01.08.2017, Art. 88 Rn. 18.
[93] *Selk* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 88, Rn. 9.
[94] Vgl. C.I.

arbeitung für Zwecke der Arbeitsorganisation, des Managements und insb. der digitalen Gestaltung des Beschäftigtenumfeldes im Rahmen der Industrie 4.0 ist § 26 BDSG-neu nicht anwendbar, so dass auf die allgemeinen Bestimmungen aus Art. 6 DSGVO zurückgegriffen werden kann.

Bei der Abgrenzung ist dabei klar zu unterscheiden, ob lediglich die Voraussetzungen des § 26 BDSG-neu nicht vorliegen, dann wäre der Anwendungsbereich des Art. 6 DSGVO nicht eröffnet, oder ob § 26 BDSG-neu schon nicht anwendbar ist. Werden also Beschäftigtendaten zu einem Zweck verarbeitet, der in engem Zusammenhang mit der Vertragsdurchführung steht, ist jedoch diese Verarbeitung nicht erforderlich, weil es beispielsweise schonendere Maßnahmen gibt oder der Eingriff unverhältnismäßig ist, so ist die Anwendung des Art. 6 DSGVO gesperrt. Werden anhand einer Datenbrille beispielsweise auch Informationen über die Sehschärfe des Beschäftigten erhoben und gespeichert, so kann man zu dem Ergebnis gelangen, dass diese Verarbeitung nach § 26 BDSG- neu nicht zulässig ist, weil diese Daten für die eigentliche Funktion der Datenbrille nicht erforderlich sind oder weil überwiegende Interessen des Beschäftigten gegen die Verarbeitung von Gesundheitsdaten sprechen. In diesem Fall kann nicht auf Art. 6 Abs. 1 f DSGVO zur Rechtfertigung der Datenverarbeitung zurückgegriffen werden.

Zum Teil wird in der Literatur[95] auch vertreten, dass die Interessenabwägungsklausel kein Auffangtatbestand sei. Neben der Vertragserfüllung[96] könne in solchen Fällen lit. f nur dann zur Anwendung kommen, wenn vertragliche Schutzpflichten nicht verletzt werden. Zwar habe die Interessenabwägung nach lit. f grundsätzlich auch bei Bestehen eines Vertragsverhältnisses weiterhin selbstständige Bedeutung, ihr Anwendungsbereich sei aber eng auszulegen. Gestützt wird diese Ansicht auf die Rechtsprechung des BAG, wonach über eine allgemeine Interessenabwägung in die Privatsphäre des Beschäftigten nicht tiefer eingedrungen werden dürfe, als es der Zweck des Arbeitsverhältnisses unbedingt erfordere.[97] Diese Ansicht verkennt jedoch zum einen die eigenständige Bedeutung des europarechtlichen Art. 6 Abs. 1 lit. f. DSGVO, für dessen Auslegung die Rechtsprechung des BAG aus dem Jahr 1986 nur bedingt tauglich ist. Zum anderen aber geht es bei der Rechtsprechung des BAG um die Rechtfertigung einer Datenverarbeitung auf der Grundlage der Vertragserfüllung, wie sie zunächst in § 32 BDSG-alt, und heute in § 26 BDSG-neu geregelt ist. Das hat nichts mit der Frage zu tun, ob und in welchem Umfang die Datenverarbeitung von Beschäftigtendaten auf die allgemeine Interessenabwägung gestützt werden kann, wenn der Zweck der Verarbeitung nicht zum Zwecke des Beschäftigtenverhältnisses i.S.d. § 26 BDSG-neu erfolgt. Richtig ist allerdings, dass vertragliche Schutzpflichten bei der Interessenabwägung berücksichtigt werden müssen.

Ein Beispiel für eine Verarbeitung von Beschäftigtendaten, die nicht im Rahmen des Arbeitsvertrags erfolgt, bietet der in der Literatur und den Aufsichtsbehörden diskutierte Fall des Nachweises der Zahlung des Mindestlohns: Bei der Beauftragung von Subunternehmern haftet der Auftraggeber für die Verpflichtung des Auftragnehmers zur Zahlung des Mindestlohns. Zur Reduzierung dieses Haftungsrisikos fordern die Auftraggeber regelmäßig Nachweise über die ordnungsgemäße Zahlung des Min-

---

[95] *Schulz,* in: Gola, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 13.
[96] Art. 6 Abs. 1 lit b DSGVO sowie § 26 BDSG-neu als spezielle Vorschrift für Arbeitsverträge.
[97] BAG, Urt. v. 22.10.1986- 5 AZR 660/85.

destlohns an ihre Beschäftigten. Dieser Praxis stehen nach bisheriger Ansicht der Datenschutzbehörden datenschutzrechtliche Bedenken entgegen. Die mit der Beibringung solcher Nachweise einhergehende Datenverarbeitung ergehe jedenfalls nicht in Ansehung der eigentlichen Zweckbestimmung, namentlich der Erfüllung von arbeitsvertraglichen Pflichten. Nach vorherrschender Auffassung der Aufsichtsbehörden soll eine Verarbeitung infolge überwiegender Interessen der Beschäftigten und der fehlenden Erforderlichkeit auch auf Grundlage der allgemeinen Interessenabwägungsklausel ausscheiden.[98] Diese Ansicht dürfte mit Art. 6 DSGVO nicht vereinbar sein.[99] Mit Einführung der Interessensabwägungsklausel auf europarechtlicher Grundlage hat man sich, wie nachfolgend aufgezeigt wird, von der strengen Verhältnismäßigkeitsprüfung des deutschen Rechts verabschiedet, um – ausgehend von der Erwartungshaltung des Beschäftigten – den berechtigten Interessen des Verantwortlichen mehr Raum zu geben.

2.2.2 Die Voraussetzungen der Interessenabwägung

Wie sich bereits aus der Bezeichnung dieses Rechtfertigungsgrundes ergibt, findet auch hier eine Interessenabwägung statt. Die Verarbeitung personenbezogener Daten ist danach dann rechtmäßig, wenn sie zur Wahrung der Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die datenschutzbezogenen Interessen, Grundrechte und Grundfreiheiten des Betroffenen nicht überwiegen. Die Norm enthält demnach die zentrale Interessenabwägungsklausel der DSGVO, der im Datenverkehr zwischen Privaten größte praktische Bedeutung zukommt.[100]

Dabei reicht es nicht aus, dass der Verantwortliche ein Interesse daran hat, Nutzen aus der Verarbeitung zu ziehen, sei es wirtschaftlicher oder ideeller Art. Vielmehr muss das Interesse an der Verarbeitung ein berechtigtes Interesse sein. Dies setzt voraus, dass die vom Verantwortlichen oder einem Dritten mit der Verarbeitung verfolgten Ziele rechtmäßig sind und im Einklang mit der Rechtsordnung des jeweiligen Mitgliedstaats und Unionsrecht stehen. Das berechtigte Interesse muss auch hinreichend konkretisiert sein, damit es mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person abgewogen werden kann.[101] Beispiele für ein berechtigtes Interesse i.S.d. Art. 6 Abs. 1 f DSGVO sind die Betrugsprävention, Direktwerbung, die Übermittlung von Kunden- und Beschäftigtendaten innerhalb einer Unternehmensgruppe sowie die Gewährleistung der Netz- und Informationssicherheit.[102] Ein berechtigtes Interesse kann sich auch aus der Wahrnehmung des Rechts auf Meinungs- und Informationsfreiheit, der Durchsetzung von Rechtsansprüchen, der

---

[98] *Gola*, in: Gola, DS-GVO, 1. Auflage 2017, Art. 6 Rn.114 unter Bezugnahme auf 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung v. 18./19.3.2015.

[99] Ausgehend von der Erwartungshaltung der Mitarbeiter der Subunternehmer überwiegt das Interesse des Auftraggebers, die Einhaltung der Mindestlohnvorschriften kontrollieren zu können. Diese müssen damit rechnen, dass im Subunternehmerverhältnis dem Auftraggeber Auskünfte erteilt werden. Ggf. ist ein entsprechender Hinweis durch den Subunternehmer erforderlich.

[100] *Albers* in: Wolff/ Brink BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 6 Rn. 45.

[101] *Heberlein* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 22.

[102] Erwägungsgrund 47 S. 6 u. 7, Erwägungsgrund 48 S. 1, Erwägungsgrund 49 S. 2.

Überwachung von Beschäftigten aus Sicherheitsgründen oder der Marktforschung ergeben.[103]

Anders als noch nach dem BDSG-alt können auch berechtigte Interessen Dritter berücksichtigt werden.

Fraglich ist, ob die Interessenabwägung der Verhältnismäßigkeitsprüfung entspricht, die im Rahmen des § 26 BDSG-neu durchzuführen ist.[104] In diesem Fall würde es keinen Unterschied machen, ob eine Verarbeitung von Beschäftigtendaten auf § 26 BDSG-neu oder auf Art. 6 Abs. 1 f DSGVO gestützt würde, da in beiden Fällen die Rechtmäßigkeit von der Interessenabwägung abhinge.

Gegen eine Entsprechung spricht zunächst, dass nach dem Willen des Gesetzgebers § 26 BDSG-neu den § 32 BDSG-alt fortführen und insb. die hierzu ergangene Rechtsprechung übernommen werden soll. Bei Art. 6 DSGVO handelt es sich demgegenüber um eine europäische Norm, die sich nicht an der Rechtsprechung des BAG orientiert, sondern vom EuGH präzisiert und ausgelegt wird.[105] Die bisher vom EuGH zur Fragen der Verhältnismäßigkeit getroffenen Entscheidungen deuten darauf hin, dass es im europäischen Rechtsverständnis keine mit dem deutschen Recht vergleichbare strukturierte Verhältnismäßigkeitsprüfung gibt.[106]

Zudem ist der Bezugspunkt unterschiedlich: Bei der Prüfung nach § 26 BDSG-neu stellt der Arbeitsvertrag den Bezugspunkt dar: Die Verarbeitung muss zur Erfüllung des Arbeitsvertrags erforderlich sein, d.h. auch auf Arbeitgeberseite können lediglich Interessen aus dem Arbeitsverhältnis in die Waagschale geworfen werden. Ein solcher Bezugspunkt fehlt bei Art. 6 Abs. 1 f DSGVO: Hier können jegliche berechtigten Interessen des Arbeitgebers denen des Beschäftigten gegenübergestellt werden.

Auch scheint die Interessenabwägung unter der DSGVO wesentlich weitgehendere Verarbeitungsmaßnahmen zu ermöglichen, als das unter § 26 BDSG-neu der Fall ist. Grundsätzlich gilt auch hier zunächst, dass je eingriffsintensiver eine Maßnahme des Arbeitgebers ist, desto eher überwiegen die Interessen des Beschäftigten. Allerdings ergibt sich bereits aus dem Wortlaut, dass die Abwägung im Zweifel nicht gegen die Verarbeitung spricht. Vielmehr bezweckt die Vorschrift, dass nur unverhältnismäßige Folgen für den Betroffenen vermieden werden sollen.[107]

---

[103] Artikel-29-Datenschutzgruppe, Stellungnahme 6/2014 zum Begriff des berechtigten Interesses (WP 217), S. 31 f.

[104] *Gola*/*Thüsing*/*Schmidt* sind der Ansicht, dass der Maßstab der Erforderlichkeit in § 26 BDSG mit dem von der DSGVO in Art. 6 Abs. 1 lit. b aufgestelltem Maßstab identisch sei, Vgl. DuD 2017, 244 (245), Was wird aus dem Beschäftigtendatenschutz?; ebenso: *Gola* in: Gola, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 95 ff.

[105] *Reimer* weist daher zurecht darauf hin, dass die Abwägungen des deutschen Datenschutzrechts nicht einfach übertragbar seien, Vgl. *Reimer* in: Sydow, DS-GVO, 1. Auflage 2017, Art. 6 Rn. 59.

[106] EuGH v. 16.12.2008 in der RS C-524/06 („Heinz Huber vs. Bundesrepublik Deutschland") – CELEX-Nummer: 62006CJ0524, Rn. 47 ff.

[107] in diesem Sinn: *Reimer* in Sydow, Datenschutzgrundverordnung, 1. Auflage 2017, Art. 6 Rn. 62; *Härting*, CR 2013, 715 (717), Datenschutzreform in Europa: Einigung im EU-Parlament; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 52.

Zudem kann die Abwägung vom Arbeitgeber beeinflusst werden. So hängt die Frage der Eingriffsintensität u.a. auch von der Erwartungshaltung des Beschäftigten ab. Nach Erwägungsgrund 47 sind bei der Abwägung die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Dabei ist auch zu prüfen, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherwiese eine Verarbeitung für diesen Zweck erfolgen wird. Muss die Person nicht mit einer Verarbeitung rechnen, überwiegen im Regelfall die Interessen und Grundrechte der betroffenen Person.

Im Beschäftigtenverhältnis ist dabei die besondere Fürsorgepflicht des Arbeitgebers zu berücksichtigen. Der Beschäftigte darf davon ausgehen, dass seine personenbezogenen Daten nur im Rahmen des Beschäftigtenverhältnisses selbst zur Erfüllung des nach dem Arbeitsvertrag Geschuldeten genutzt werden. Mit einer weitergehenden Verarbeitung zu Zwecken außerhalb des Beschäftigtenkontextes muss der Beschäftigte nicht rechnen.

Diese Erwartungshaltung kann der Arbeitgeber jedoch durch ein hohes Maß an Transparenz beeinflussen. Wird ein Beschäftigter in einem digitalisierten Arbeitsumfeld eingesetzt, in dem nicht nur seine konkrete Tätigkeit, sondern ggf. das gesamte Unternehmen „digital gesteuert“ wird, so muss der Beschäftigte damit rechnen, dass auch seine personenbezogenen Daten verarbeitet werden. Um derartige Verarbeitungsschritte auf die Interessenabwägung stützen zu können, ist es erforderlich, dem Beschäftigten vor Beginn seiner Tätigkeit im Einzelnen Funktionsweisen und Datenverarbeitungsvorgänge zu erläutern. Je stärker der Beschäftigte selbst in die Datenverarbeitung einbezogen ist, und je besser sein Verständnis für die Zusammenhänge zwischen Arbeitsfunktionen und Datenverarbeitungen ausgeprägt ist, desto eher wird man davon ausgehen können, dass der Beschäftigte mit einer Verarbeitung auch seiner personenbezogenen Daten rechnen muss. Beschäftigte, die Tätigkeiten ausüben, die nur wenig mit digitalen Vorgängen zu tun haben, und die selbst daher auch wenig Verständnis für derartige Verarbeitungsvorgänge haben, müssen demgegenüber auch dann nicht mit einer Verarbeitung ihrer personenbezogenen Daten rechnen, wenn ihnen die Funktionszusammenhänge erläutert werden.

Insgesamt enthält die Anwendung der Interessensabwägungsvorschrift erhebliche Rechtsunsicherheiten, die erst durch Entscheidungen des EUGH geklärt werden können.[108]

2.2.3 Anwendungsbeispiele

Wir hatten oben festgestellt, dass einige Industrie 4.0 Anwendungen nicht unter § 26 BDSG-neu fallen, weil die Datenerfassung nicht im direkten Zusammenhang mit dem Beschäftigtenverhältnis steht. Es ist daher zu prüfen, ob derartige Anwendungen durch die Interessenabwägung nach Art. 6 Abs. 1 f DSGVO gerechtfertigt sein können.

---

[108] diese Rechtsunsicherheit wird bemängelt bspw. von *Roßnagel*/*Nebel*/*Richter*, ZD 2015, 455 (457), Was bleibt vom Europäischen Datenschutzrecht?

Auch Art. 6 Abs. 1 f verlangt zunächst, dass die Datenverarbeitung zu einem konkreten Zweck erfolgt. Das Sammeln von Beschäftigtendaten, um hieraus Muster und Verhaltensweisen abzuleiten, die dann als Grundlage für etwaige organisatorische Maßnahmen dienen können, wäre danach auch unter Art. 6 Abs. 1 f unzulässig. Derartige Big Data Anwendungen dürfen nur mit anonymisierten Daten durchgeführt werden.

Adaptive Assistenzsysteme und Industrie 4.0 Anwendungen, die hingegen einem konkreten Zweck dienen, ohne dass der Zweck im Arbeitsverhältnis begründet liegt, können unter Art. 6 Abs. 1 f gerechtfertigt sein. Soll beispielsweise anhand von Daten die Beziehung zu Lieferanten oder Kunden organisiert werden, könnten derartige Datenverarbeitungsvorgänge als im überwiegenden Interesse des Arbeitgebers gerechtfertigt sein. Aber auch wenn derartige Datenverarbeitungen im Interesse des Lieferanten oder Kunden erfolgen, kommt Art. 6 Abs. 1 f in Betracht.

2.2.4 Widerspruchsrecht

Erfolgt die Verarbeitung der personenbezogenen Daten des Beschäftigten ausschließlich[109] auf Grundlage einer Interessenabwägung (s. oben), ist jedoch das Widerspruchsrecht zu berücksichtigen. Gem. Art. 21 Abs. 1 DSGVO kann der Beschäftigte losgelöst von Fristen, wenn auch nur unter engen inhaltlichen Voraussetzungen, der weiteren Verarbeitung widersprechen. Die Ausübung des Widerspruchsrechts setzt voraus, dass der Beschäftigte Gründe geltend machen kann, die sich aus seiner besonderen Situation ergeben, die gegen eine weitere Datenverarbeitung sprechen. Weitere Voraussetzung ist, dass der Verantwortliche seinerseits keine zwingenden und schutzwürdigen Gründe für die Verarbeitung nachweisen kann, die im Vergleich zu den Interessen, Rechten und Freiheiten des Beschäftigten überwiegen. Auch hier ist also eine Interessenabwägung vorzunehmen. In Abgrenzung zu Art. 6 Abs. 1 lit. f. DSGVO ist dabei jedoch keine objektiv typisierende Ex-ante Betrachtung, sondern vielmehr eine Einzelfallbetrachtung vorzunehmen. Der Beschäftigte muss daher konkrete Tatsachen vortragen und ggf. nachweisen, die in Bezug auf seine besondere Situation und Person ausnahmsweise eine weitere Verarbeitung seiner personenbezogenen Daten[110] unrechtmäßig erscheinen lassen.

Die spezifische individuelle Situation des Beschäftigten kann sich aus besonderen rechtlichen, sozialen, wirtschaftlichen oder gesellschaftlichen Zwangssituationen oder damit vergleichbaren atypischen Umständen ergeben, welche i.R.d. abstrakt-generellen Interessenabwägung nicht erfasst wurden.[111] Als Beispiel wird etwa der Fall angeführt, dass die Gesundheitsdaten eines Patienten anlässlich einer Operation in einem Krankenhaussystem gespeichert wurden und ein Verwandter des Patienten eine Führungsposition in diesem Krankenhaus übernehmen soll. [112] Ein gleichwohl umstrittenes Beispiel aus dem Beschäftigtendatenschutz beschreibt die Situation eines Beschäftigten, der der weiteren Speicherung seiner früheren Fehlzei-

---

[109] *Martini* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 21 Rn. 28.

[110] *Kamann/Braun* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 21 Rn. 16, die jedoch in Ausnahmefällen auch einen indirekten Personenbezug genügen lassen wollen, Rn. 17.

[111] *Schulz* in: Gola, DS-GVO, 1. Auflage. 2017, Art. 21 Rn. 9; *Kamann/Braun* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 21, Rn. 20; *Martini* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 21 Rn. 30.

[112] *Kamann/Braun* in: Ehmann/Selmayr, DS-GVO, 1. Aufl. 2017, Art. 21 Rn. 20, m.w.N.

ten widerspricht, weil sein ärztliches Attest zum Gegenstand von Kantinengesprächen gemacht worden ist.[113]

Die Gründe, welche sich aus der besonderen Situation des Beschäftigten ergeben, können sowohl in dadurch veränderten Umständen in der Person des Beschäftigten, als auch in einer sich (nachträglich) verändernden Eingriffsqualität oder einer so geschaffenen (neuen) Gefahrenlage liegen.[114]

2.3 Regelung durch Kollektivvereinbarungen

2.3.1 Hintergrund

Die DSGVO und das BDSG-neu sehen die Möglichkeit vor, im Rahmen von Kollektivvereinbarungen spezifische Vorschriften zum Beschäftigtendatenschutzrecht zu schaffen. Solche Vereinbarungen bieten den Vorteil, dass die Betriebsparteien mit Blick auf die konkrete Situation im Unternehmen passgenau zugeschnittene Regelungen zum Datenschutz treffen können. Zudem können im Rahmen von Kollektivvereinbarungen ein angemessener Ausgleich der divergierenden Interessen von Arbeitgebern und Beschäftigten geschaffen und damit Rechtsunsicherheiten bei der Verarbeitung von Beschäftigtendaten reduziert werden. Kollektivvereinbarungen können daher auch geeignete Regelungsinstrumente für den Einsatz adaptiver Assistenzsysteme sein.

2.3.2 Kollektivvereinbarungen als Erlaubnistatbestand

Im Laufe des Gesetzgebungsverfahrens war zunächst umstritten, ob auch Betriebsvereinbarungen als datenschutzrechtliche Erlaubnistatbestände in Betracht kommen sollten. Auf deutsche Initiative wurde jedoch eine entsprechende Regelung in Art. 88 DSGVO aufgenommen. Nach Art. 88 Abs. 1 DSGVO können Kollektivverträge „spezifischere Vorschriften“ für den Beschäftigtendatenschutz vorsehen. Voraussetzung ist allerdings, dass das nationale Recht kollektivvertragliche Regelungen im Bereich des Beschäftigtendatenschutzes zulässt.[115] Der deutsche Gesetzgeber hat von dieser Regelungsbefugnis Gebrauch gemacht und in § 26 Abs. 4 S. 1 BDSG-neu eine entsprechende Rechtsgrundlage geschaffen. Nach § 26 Abs. 4 S. 1 BDSG-neu können danach auch Kollektivvereinbarungen Grundlage für die Verarbeitung personenbezogener Beschäftigtendaten sein. Unter den Begriff der Kollektivvereinbarung fallen nach der Legaldefinition in § 26 Abs. 1 S. 1 BDSG-neu Tarifverträge sowie Tarif- und Dienstvereinbarungen. § 26 Abs. 4 BDSG-neu steht damit im Einklang mit der bisherigen Rechtsprechung des BAG, nach der Tarifverträge und Betriebsvereinbarungen als „andere Rechtsvorschriften“ i.S. des § 4 Abs. 1 BDSG und damit ebenfalls als zulässige Verarbeitungsgrundlage einzuordnen waren.

---

[113] *Däubler*, Gläserne Belegschaften, 7. Auflage 2017, Rn. 565; a.A. *Kamann/Braun* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 21, Rn. 20, der darauf verweist, dass die Vorbeugung einer sich möglicherweise wiederholenden Datenschutzverletzung keine Sondersituation in diesem Sinne darstellen solle.

[114] *Schulz* in: Gola, DS-GVO, 1. Auflage 2017, Art. 21 Rn. 9.

[115] *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand 01.08.2017, Art. 88, Rn. 49.

2.3.3 Anforderungen an eine Kollektivvereinbarung im Bereich des Beschäftigtendatenschutzes

Soll eine Kollektivvereinbarung die Grundlage für die Verarbeitung von Beschäftigtendaten darstellen, müssen künftig folgende Anforderungen berücksichtigt werden:

2.3.3.1 Verarbeitung für Zwecke des Beschäftigungsverhältnisses

Nach § 26 Abs. 4 Satz 1 BDSG-neu muss die in der Kollektivvereinbarung geregelte Verarbeitung für Zwecke des Beschäftigungsverhältnisses[116] erfolgen. Die kollektivvertragliche Regelung muss also mit der Einstellung, Erfüllung und Beendigung eines Beschäftigungsverhältnisses in Zusammenhang stehen. Nach dem Betriebsverfassungsgesetz kommt den Vertragsparteien dabei grundsätzlich eine weitreichende Regelungskompetenz zu. Datenschutzrechtliche Kollektivvereinbarungen können daher etwa Regelungen zu folgenden Aspekten enthalten:[117]

- allgemeine personelle Angelegenheiten §§ 92 ff. BetrVG,
- Berufsbildung, §§ 96 ff. BetrVG,
- Gestaltung von Arbeitsplatz, Arbeitsablauf und Arbeitsumgebung, §§ 90 f. BetrVG,
- betriebliche Ordnung, § 87 Abs. 1 Nr. 1 BetrVG,
- technische Überwachungseinrichtungen, § 87 Abs. 1 Nr. 6 BetrVG,
- Sozialeinrichtungen, § 87 Abs. 1 Nr. 8 BetrVG.

2.3.3.2 Verweis auf Anforderungen in Art. 88 Abs. 2 DSGVO

Bei der Ausgestaltung eines auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes im Rahmen von Kollektivvereinbarungen müssen die Verhandlungsparteien gemäß § 26 Abs. 4 Satz 2 BDSG-neu die in Art. 88 Abs. 2 DSGVO geregelten Grundsätze beachten.

2.3.3.2.1 Grundrechte und berechtigte Interessen der Beschäftigten

Nach Art. 88 Abs. 2 DSGVO müssen Kollektivvereinbarungen die menschliche Würde sowie die berechtigten Interessen und Grundrechte der betroffenen Person wahren. Die DSGVO formuliert damit Mindestanforderungen, die auch in Rahmen von Kollektivvereinbarungen zu berücksichtigen sind. Der materielle Regelungsgehalt der Vorschrift ist allerdings unklar, da die Pflicht zur Beachtung der Grundrechte und berechtigten Interessen der betroffenen Personen bereits aus den allgemeinen Vorgaben des Europa- und Verfassungsrechts folgt.[118] So verpflichtet etwa § 75 BetrVG die Betriebsparteien zur Wahrung der Freiheits- und Gleichheitsrechte der Beschäftigten. Datenschutzrechtliche Regelungen, die diesem Standard nicht gerecht werden, verstoßen zugleich gegen materielle Schutzvorschriften der DSGVO und können daher nicht als Verarbeitungsgrundlage herangezogen werden. Die Regelung in

---

[116] Vgl. zu § 26 Abs. 1 BDSG-neu oben Ziff. I.
[117] *Imping*, CR 2017, 378 (380).
[118] *Maschmann*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 42; *Tiedemann*, in: Sydow, Europäische Datenschutzgrundverordnung. 1. Auflage 2017, Art. 88 Rn. 19.

Art. 88 Abs. 2 DSGVO wird man vor diesem Hintergrund als deklaratorische Bestimmung verstehen können, mit der einzelne Aspekte des Betroffenenschutzes exemplarisch hervorgehoben werden.[119]

2.3.3.2.2 Transparenz der Verarbeitung

Durch die Formulierung „insbesondere im Hinblick auf die Transparenz der Verarbeitung“ betont Art. 88 Abs. 2 DSGVO zudem, dass die Vertragsparteien bei der Ausgestaltung kollektivvertraglicher Regelungen zum Beschäftigtendatenschutz den Transparenzgrundsatz zu beachten haben. Auch auf Grundlage von Kollektivvereinbarungen dürfen Daten daher nur in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.[120] Im Rahmen von Betriebsvereinbarungen kann diesen Vorgaben etwa durch Regelung konkreter Informationspflichten Rechnung getragen werden. Die Transparenz kann zudem durch verständliche Beschreibung der Datenverarbeitung im Rahmen von Betriebsvereinbarungen erhöht werden. Zudem ist es möglich, die Beschäftigtenvertreter (Betriebsrat) als Informationsintermediäre zu nutzen.[121]

2.3.3.2.3 Mögliche Regelungsgegenstände

Die Regelung in Art. 88 Abs. 2 DSGVO nennt verschiedene Verarbeitungsvorgänge, zu denen die Vertragsparteien Regelungen in Kollektivvereinbarungen treffen können. Mögliche Reglungsgegenstände sind danach die Übermittlung von Daten innerhalb einer Unternehmensgruppe sowie die Einrichtung von Systemen zur Überwachung am Arbeitsplatz. Die Auflistung ist nicht abschließend („insbesondere“). Vielmehr sind Vereinbarungen zu allen Aspekten des Beschäftigungskontextes denkbar. In der Literatur werden etwa kollektivvertragliche Regelungen zu Zweckbindung, Löschfristen, Datensicherheit, Datenpannen, Datenschutz-Folgenabschätzung sowie Dokumentations- und Rechenschaftspflichten vorgeschlagen.[122]

2.3.3.3 Vorgegebener Mindeststandard?

Noch nicht abschließend geklärt ist, in welchem Umfang die Vertragsparteien im Rahmen von Kollektivvereinbarungen von dem durch die DSGVO vorgegebenen Schutzstandard abweichen dürfen. Die Öffnungsklausel in Art. 88 Abs. 1 DSGVO ermöglicht die Vereinbarung „spezifische Vorschriften“ in Kollektivvereinbarungen. Mit dieser Formulierung bringt der Verordnungsgeber zum Ausdruck, dass auch derartige Vereinbarungen nicht beliebig von den Vorgaben der DSGVO abweichen dürfen.[123] Vielmehr sind nach der ganz überwiegenden Ansicht in der Literatur kollektivvertragliche Regelungen ausgeschlossen, die eine Absenkung des Datenschutzes unter das Schutzniveau der DSGVO zur Folge haben.[124] Was dies im Einzelfall be-

---

[119] *Selk*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 115.
[120] vgl. zum Transparenzgrundsatz näher unter E.III.
[121] So *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 88 Rn. 87; In diese Richtung auch Wybitul, ZD 2016, 203 (208).
[122] S. hierzu insgesamt Wybitul, ZD 2016, 203 (208 f).
[123] *Pauly*, in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 4.
[124] *Tiedemann*, in: Sydow, Europäische Datenschutzgrundverordnung, 1. Auflage 2017, Art. 88 Rn. 18; *Selk*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 80; *Pötters*, in: Gola, DS-GVO, 1. Auflage 2017, Art. 88, Rn. 20.

deutet, wo also die Grenze zwischen noch erlaubter Konkretisierung und bereits verbotener Unterschreitung des Schutzniveaus genau gezogen werden muss, ist allerdings noch ungeklärt. Im BSDG-neu wird in § 26 Abs. 5 lediglich festgelegt, dass der Verantwortliche geeignete Maßnahmen ergreifen muss, um sicherzustellen, dass die in Art. 5 DSGVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Zudem dürften die besonderen Anforderungen beim Umgang mit sensiblen Daten nach Art. 9 DSGVO, die Grundpflichten des Verarbeiters nach Art. 13 ff. DSGVO und die grundlegenden Rechte der Betroffenen, zu denen insbesondere das Auskunftsrecht nach Art. 15 DSGVO und die Rechte auf Berichtigung bzw. Löschung nach Art. 16 ff. DSGVO zählen, zu diesem nicht disponiblen Kernbestand gehören.[125] Das Mindestschutzniveau wäre also beispielsweise dann nicht mehr gewahrt, wenn in Kollektivvereinbarungen Betroffenenrechte des Beschäftigten eingeschränkt oder sogar ausgeschlossen werden.

Größerer Gestaltungspielraum besteht hingegen bei der Regelung konkreter Verarbeitungsvorgänge. Zwar dürfen auch Verarbeitungsgrundlagen, die die Parteien im Rahmen einer Kollektivvereinbarung regeln, das Recht auf informationelle Selbstbestimmung der Beschäftigten nicht in unverhältnismäßiger Weise beschränken. Maßgeblich ist also auch insoweit eine Abwägung der verschiedenen Rechtspositionen.[126] Im Rahmen dieser Abwägung ist allerdings zu berücksichtigen, dass Regelungen in Kollektivvereinbarungen in einem auf Interessenausgleich ausgerichteten Verfahren zwischen den Vertragsparteien auf Arbeitgeber- und Beschäftigtenseite ausgehandelt werden. Vor diesem Hintergrund spricht eine gewisse Vermutung dafür, dass datenschutzrechtliche Regelungen in Kollektivvereinbarungen als Ergebnis eines solchen Aushandlungsprozesses einen angemessenen Ausgleich zwischen den divergierenden Interessen von Arbeitgebern und Beschäftigten schaffen und damit nicht hinter dem Mindestschutzniveau der DSGVO zurück bleiben. Allerdings kann nicht ausgeschlossen werden, dass die Regelung konkreter Verarbeitungsgrundlagen in Kollektivvereinbarungen die Rechte der Beschäftigten in unverhältnismäßiger Weise beschränkt und damit zu einer unzulässigen Unterschreitung des Mindestschutzniveaus führt. In welchen Konstellationen von einer solchen Unterschreitung auszugehen ist, wird letztlich der EuGH zu klären haben.

2.3.4 Betriebsvereinbarungen als Verarbeitungsgrundlage für die Datenverarbeitung beim Einsatz von adaptiven Arbeitsassistenzsystemen?

Im Rahmen von Kollektivvereinbarungen können die Vertragsparteien anlassbezogen und auf den jeweiligen Einzelfall abgestimmte Rechtsgrundlagen für die Verarbeitung von Beschäftigtendaten schaffen. Im Unterschied zu den gesetzlichen Erlaubnistatbeständen haben Betriebsvereinbarungen den Vorteil, dass die Beteiligten sehr viel konkreter festlegen können, unter welchen Voraussetzungen der Arbeitgeber personenbezogene Daten für betriebliche Zwecke verarbeiten darf. Gerade in Konstellationen, in denen als Verarbeitungsgrundlage grundsätzlich nur die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO in Betracht kommt, verbleiben häufig Unsicherheiten. Durch präzisierende Regelungen in Kollektivvereinbarungen

---

[125] Vgl. zu dieser Umgrenzung des Kernbestands etwa *Düwell/ Brink* NZA 2016, 665, 666 f.

[126] Zu der insoweit vorzunehmenden Abwägung näher *Maschmann*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 84.

können solche Rechtsunsicherheiten erheblich reduziert werden.[127] Aus Arbeitgebersicht wird daher häufig ein Interesse an einer entsprechenden Vereinbarung bestehen. Gleichzeitig bietet das Instrument der Kollektivvereinbarung den Vertretungsgremien auf Beschäftigtenseite die Möglichkeit, gestaltend zur Wahrung der Interessen der von ihm vertretenen Belegschaft beizutragen.[128]

Vor diesem Hintergrund kann es sich anbieten, auch den Einsatz adaptiver Arbeitsassistenzsysteme und die damit zusammenhängende Datenverarbeitung in Kollektivvereinbarungen zu regeln. Inhaltlich sollte dabei ein hohes Maß an Transparenz hinsichtlich des Umgangs mit Daten des Beschäftigten angestrebt werden. Aus der kollektivvertraglichen Regelung muss klar hervorgehen, welche personenbezogenen Daten im Rahmen des eingesetzten Systems erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden. Dies setzt hinreichend detaillierte und verständliche Regelungen voraus. Je nach eingesetztem System sollte dabei auf folgende Aspekte eingegangen werden:[129]

- Kreis der Betroffenen,
- Bestimmung der grundrechtlichen Position der Beteiligten,
- Beschreibung der Verfahrensabläufe sowie Vorkehrungen zur Datensicherheit sowie zur Protokollierung,
- Komponenten des Systems (z.B. Hardware, Betriebssystem, Applikationen, vor- und nachgelagerte Datenbanken, interne und externe Schnittstellen, wie z.B. Archivsysteme etc.),
- Katalog der betroffen Beschäftigtendaten,
- ggf. Schnittstellen (Import/Export von Beschäftigtendaten);
- Überblick über Zugriffsrechte (evtl. Informationen zu Rollenbeschreibungen des Berechtigungskonzepts),
- im Falle von Datenübermittlung (z.B. an verbundene Unternehmen): Auflistung der Datenempfänger mit jeweiligen Nutzungszwecken.

Aus der Regelung sollte außerdem erkennbar sein, zu welchem Zweck adaptive Assistenzsysteme im Unternehmen eingesetzt werden sollen.

2.4 Die Einwilligung als Verarbeitungsgrundlage

2.4.1 Regelung in der DSGVO

Die Einwilligung als Verarbeitungsgrundlage ist in Art. 6 Abs. 1 lit. a DSGVO geregelt. Für die Verarbeitung besonderer Kategorien personenbezogener Daten enthält Art. 9 Abs. 2 lit. a DSGVO eine gesonderte Einwilligungsregelung.

Die Einwilligung ist eine Willenserklärung, mit der der Betroffene auf Grund einer privatautonom getroffenen Entscheidung dem Verarbeiter die Verarbeitung seiner per-

---

[127] So zutreffend *Selk*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 74.
[128] *Selk*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 74.
[129] Vgl. *Conrad*, Recht des Datenschutzes, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2. Auflage 2016, S. 1637.

sonenbezogenen Daten gestattet.[130] Ob eine autonome Entscheidung in Abhängigkeitsverhältnissen wie dem Arbeitsverhältnis überhaupt getroffenen werden kann, ist seit langem umstritten. Bei den Verhandlungen um die DSGVO gab es daher zunächst Überlegungen, die Einwilligung als Erlaubnis für die Verarbeitung personenbezogener Beschäftigtendaten generell auszuschließen. So hieß es etwa in einer früheren Entwurfsfassung der Kommission:

„Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht."[131]

Eine derart weitreichende Einschränkung konnte sich in den weiteren Verhandlungen allerdings nicht durchsetzen. Nachdem der entsprechende Passus bereits in der Fassung des Europäischen Parlaments gestrichen wurde, sollte die generelle Möglichkeit von Einwilligungen im Beschäftigungskontext nach dem Willen des Rats sogar positiv im Verordnungstext aufgenommen werden.[132]

In der finalen Fassung der DSGVO ergibt sich die Zulässigkeit von Beschäftigteneinwilligungen jedenfalls aus dem Erwägungsgrund 155 DSGVO. Danach sollen Mitgliedstaaten auf Grundlage der Öffnungsklausel in Art. 88 DSGVO Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung verarbeitet werden dürfen, erlassen können. Der europäische Gesetzgeber bringt damit zum Ausdruck, dass Betroffene auch in Abhängigkeitsverhältnissen wie dem Arbeitsverhältnis privatautonome Entscheidungen über die Verarbeitung ihrer Daten treffen können.[133]

Die Einwilligung kann damit auch unter der DSGVO eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten in Arbeitsverhältnissen bilden.

2.4.1.1 Ergänzende Regelung in § 26 Abs. 2 BDSG-neu

§ 26 Abs. 2 BDSG-neu hat die Voraussetzungen, unter denen eine Einwilligung im Beschäftigtenkontext erteilt werden kann, weiter konkretisiert. Diese Regelung ist somit ergänzend zu Art. 6 Abs. 1 lit. a DSGVO heranzuziehen.

2.4.2 Wirksamkeitsvoraussetzungen

Nach Art. 4 Nr. 11 DSGVO bezeichnet die Einwilligung der betroffenen Person

„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeu-

---

[130] *Albers* in: Wolff/Brink BeckOK Datenschutzrecht, 21. Edition, Stand: 01.08.2017, Art. 6 DSGVO Rn. 19.

[131] S. zu dieser Formulierung von Art. 7 Abs. 4 DSGVO-E(KOM) und anderen Entwurfsfassungen der Kommission *Frenzel* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 4.

[132] *Pauly* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 88 Rn. 8.

[133] *Maier,* DuD 2017, 169 (172); *Wybitul* NZA 2017, 413 (416); *Schnatz,* NJW 2016, 1841 (1845); *Heckmann/Paschke*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 47; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 512; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 6.

tigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist."

Unter welchen Bedingungen eine Einwilligung als zulässige Rechtsgrundlage für die Datenverarbeitung abgegeben werden kann, ist in Art. 7 DSGVO geregelt. Zu den Bedingungen gehören die Freiwilligkeit, die Zweckbindung, die Bestimmtheit, die Transparenz und die Einhaltung der Formerfordernisse.

Ergänzt werden diese Voraussetzungen durch die Anforderungen in § 26 Abs. 2 BDSG-neu.

2.4.2.1 Freiwilligkeit

Eine wirksame Einwilligung des Betroffenen liegt nur vor, wenn dieser sich freiwillig entschlossen hat, die Verarbeitung seiner Daten zu gestatten. Unter welchen Voraussetzungen von einer freien Wahl der betroffenen Person angenommen werden kann, wird in der DSGVO nicht ausdrücklich geregelt. Aus Erwägungsgrund 42 S. 5 DSGVO folgt, dass der Betroffene grundsätzlich in der Lage sein muss, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

Neben Drohung und Zwang können externe Faktoren die Willensbildung beeinflussen. So wird sich der Betroffene bei seiner Entscheidung häufig von finanziellen oder sozialen Anreizen leiten lassen. Derartige Entscheidungsfaktoren lassen die aus rechtlicher Sicht erforderliche Willensentschließungsfreiheit nicht per se entfallen.[134] Vielmehr ist im Einzelfall zu untersuchen, ob Beschränkungen der Entscheidungsfreiheit nach dem Regelungszweck der DSGVO auch rechtlich relevant sind und einer freiwilligen Entscheidung entgegenstehen.[135] Für den Beschäftigungskontext gibt es im Wesentlichen drei Kriterien für die Prüfung der Freiwilligkeit:

- die Einwilligung darf nicht von anderen Leistungen abhängig gemacht werden,
- die Einwilligung darf sich nicht auf voneinander unabhängige Verarbeitungssituationen beziehen,
- es ist anhand von Indizien festzustellen, dass das ungleiche Machtverhältnis im konkreten Fall nicht vom Arbeitgeber missbraucht wurde.

2.4.2.1.1 Keine unzulässige Koppelung

Nach Art. 7 Abs. 4 DSGVO ist bei der Beurteilung der Freiwilligkeit besonders zu berücksichtigen, ob die Erfüllung eines Vertrags von der Einwilligung in die Datenverarbeitung abhängig gemacht wurde, obwohl diese für die Vertragserfüllung nicht erforderlich ist. An einer freiwilligen Einwilligung fehlt es, wenn der Betroffene einer nicht erforderlichen Datenverarbeitung zustimmen muss, um eine vertragliche Leistung zu

---

[134] Die Annahme der grundsätzlichen Entschließungsfreiheit des Betroffenen ist damit zentrales Element der juristischen Bewertung. Zur wissenschaftlichen Kritik an dieser „Fiktion" vgl. *Simitis*, in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 4a Rn. 3 m.w.N.

[135] S. zu dieser Unterscheidung *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 12; s. auch *Ingold*, in: Sydow, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 26.

erhalten.[136] Mit dem Kopplungsverbot will der Gesetzgeber Geschäftsmodelle nach dem Prinzip „Dienstleistung gegen Daten“ verhindern oder zumindest einschränken.[137] Im Beschäftigungskontext ist Art. 7 Abs. 4 DSGVO einschlägig, wenn Vorteile wie die Einstellung, Beförderung oder Weiterbeschäftigung von der Einwilligung in eine Datenverarbeitung abhängig gemacht werden, obwohl diese mit dem eigentlichen Beschäftigungsverhältnis in keinem Zusammenhang steht.[138] Macht der Arbeitgeber den Abschluss des Arbeitsvertrags etwa davon abhängig, dass der Beschäftigte in die Veröffentlichung seines Fotos auf der firmeneigenen Website zustimmt, so liegt ein Verstoß gegen das Kopplungsverbot vor. Die Veröffentlichung kann in diesem Fall nicht auf eine wirksame Einwilligung des Beschäftigten gestützt werden.

2.4.2.1.2 Keine Globaleinwilligung

In Erwägungsgrund 43 S. 2 DSGVO wird der Koppelungsgedanke um eine Variante erweitert. Danach gilt eine Einwilligung auch dann als nicht freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl die Verarbeitungsvorgänge voneinander unabhängig sind. Ziel dieser Einschränkung ist es, die Entscheidungsmöglichkeiten des Betroffenen zu stärken, indem der Verantwortliche zu differenzierten Einwilligungserklärungen gezwungen wird.[139] Von einer unzulässigen Globaleinwilligung im Beschäftigungskontext ist etwa auszugehen, wenn der Beschäftigte die Nutzung seiner Daten für den Einsatz arbeitsunterstützender Smart Devices sowie für die Nutzung eines Systems zur Leistungsüberwachung nur als Ganzes akzeptieren kann.

2.4.2.1.3 Kein unzulässiger Druck

An der erforderlichen Freiwilligkeit der Einwilligung fehlt es weiter dann, wenn der Einwilligende bei seiner Entscheidung in unangemessener Weise unter Druck gesetzt wird. Gerade im Arbeitsverhältnis sind Situationen denkbar, in denen aufgrund einer Zwangslage des Beschäftigten von einer freiwilligen Entscheidung nicht mehr ausgegangen werden kann.[140] In Erwägungsgrund 43 S. 1 DSGVO wird ein „klares Ungleichgewicht“ zwischen der betroffenen Person und dem Verantwortlichen als Fall aufgeführt, in der die Einwilligung mangels Freiwilligkeit keine Rechtsgrundlage darstellen soll.

2.4.2.1.3.1 Keine überwiegenden Nachteile für die Betroffenen

Wie bereits erörtert, schließen strukturelle Machtungleichgewichte der Beteiligten im Beschäftigungskontext die Freiwilligkeit einer Einwilligungserklärung allerdings nicht

---

[136] *Stemmer* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, DSGVO Art. 7 Rn. 40; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 46.

[137] *Dammann,* ZD 2016, 307 (311); *Schnatz,* NJW 2016, 1841 (1845); *Stemmer* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, DSGVO Art. 7 Rn. 46.1; *Frenzel* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 21; *Ingold*, in: Sydow, DS-GVO, 1. Auflage 2017, DSGVO, Art. 7 Rn. 33.

[138] Vgl. *Taeger/Rose,* BB 2016, 819 (820).

[139] *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 1. Auflage 2017, Rn. 517.

[140] *Thüsing*, Ergonomie im Spannungsfeld von Arbeits-, Daten- und Diskriminierungsschutz, S. 38. S. zur Gefährdung der Freiwilligkeit durch Machtasymmetrie auch *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 14.

per se aus. Gleiches gilt für Einwilligungen im Verhältnis zwischen Unternehmer und Verbraucher oder zwischen Bürger und Behörde. An einer freiwilligen Einwilligung fehlt es aber, wenn der Arbeitgeber das Machtgefälle ausnutzt, um den Beschäftigten zur Einwilligung in eine Datenverarbeitung zu drängen.

Ein Indiz für eine unangemessene Drucksituation liegt vor, wenn der Beschäftigte in eine Datenverarbeitung einwilligt, die für ihn mit nicht nur unerheblichen Nachteilen verbunden ist.[141] In diesem Fall wird der Nachweis, dass die Einwilligung ohne externen Druck erfolgte, nur ausnahmsweise möglich sein.[142] Dieser Gedanke kommt auch in Erwägungsgrund 42 zum Ausdruck, wonach die Verweigerung einer Einwilligung nicht zu „Nachteilen" für die betroffene Person führen darf. Einen in diesem Sinne erheblichen Nachteil wird man allerdings erst bei schwerwiegenden Folgen für die betroffene Person annehmen können, nicht aber bereits bei bloßen Unannehmlichkeiten.[143] Ein erheblicher Nachteil dürfte etwa regelmäßig vorliegen, wenn die Einwilligung zur Voraussetzung für eine Gehaltserhöhung gemacht wird. Die Freiwilligkeit wird im Regelfall auch dann fehlen, wenn der Beschäftigte ohne Einwilligung an einen anderen Arbeitsplatz versetzt wird, es sei denn, dieser ist in jeder Hinsicht als gleichwertig anzusehen.

Dient die Datenverarbeitung gemeinsamen Interessen von Arbeitgeber und Beschäftigten oder ist sie für den Beschäftigten sogar mit Vorteilen verbunden, so spricht dies für die Freiwilligkeit einer entsprechenden Einwilligung.[144] Als Beispiele werden in der Literatur freiwillige Zusatzleistungen der Arbeitgeber genannt, etwa die Aufnahme in konzernweite Personalentwicklungssysteme oder die Einführung eines betrieblichen Gesundheitssystems. Eine entsprechende Interessenlage dürfte auch bei der Vergabe von Firmenrabatten oder der Nutzung von Fotoaufnahmen für den Internetauftritt vorliegen. Nach einem weiteren Praxisbeispiel soll die Freiwilligkeit eines Beschäftigten vermutet werden können, wenn dieser in die Datenverarbeitung einwilligt, um eine personalisierte Magnetkarte zu erhalten, mit der er die Schranke zu einem Beschäftigtenparkplatz öffnen kann, solange diese Daten nicht zu einer Anwesenheitskontrolle genutzt werden.[145]

2.4.2.1.3.2Weitere Indizien

Neben gleichgelagerten Interessen und Vorteilen für den Beschäftigten können auch andere Indizien darauf hindeuten, dass sich die strukturelle Machtdisparität im Beschäftigungskontext im konkreten Fall nicht auf die Freiwilligkeit der Einwilligung eines Beschäftigten ausgewirkt hat. Ein wichtiger Anhaltspunkt ist der Zeitpunkt der

---

[141] *Wybitul* NZA 2017, 413 (416); *Thüsing,* BB 2016, 2165 (2166); *Stemmer* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, DSGVO Art. 7 Rn. 50; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 54.

[142] Vgl. *Ernst,* ZD 2017, 110 (112); *Stelljes,* DuD 2016, 787 (788); *Spelge,* DuD 2016, 775 (780); *Härting,* ITRB 2016, 36 (39 f).

[143] *Schulz*, in: Gola, DS-GVO, 1. Auflage 2017, Art. 7, Rn. 26.

[144] *Wybitul* NZA 2017, 413 (416); *Braun,* Intelligentes Energiemanagement im Unternehmen, 129 (136).

[145] Vgl. zu diesen Beispielen *Ernst,* ZD 2017, 110 (112); *Taeger/Rose* BB 2016, 819 (822); *Stemmer* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, DSGVO Art. 7 Rn. 48; *Ingold*, in: Sydow, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 28; *Gola*, BB 2017, 1462 mit weiteren Beispielen.

Einwilligung: So besteht etwa vor Abschluss eines Arbeitsvertrages für den Betroffenen ein größerer Druck, in eine vom zukünftigen Arbeitgeber angeregte Datenverarbeitung einzuwilligen. Umgekehrt kann es als Indiz für die Freiwilligkeit dienen, wenn die Einwilligung erst nach einer verbindlichen Begründung des Arbeitsverhältnisses erklärt wurde.[146] Ein weiterer Anhaltspunkt ist, ob der Beschäftigte ausreichend Zeit für seine Einwilligungsentscheidung hatte und ob er hierzu Rücksprache mit Dritten halten konnte. Wurde die Einwilligung hingegen in einer Überrumpelungssituation abgegeben, spricht dies in aller Regel gegen die Freiwilligkeit. Schließlich soll die Bestätigung des Einwilligungstexts durch den Betriebsrat positiv zu berücksichtigen sein.[147]

2.4.2.2 Zweckbindung und Bestimmtheit

Art. 6 Abs. 1 Satz 1 lit. a DSGVO sieht vor, dass eine Einwilligung „für eine oder mehrere bestimmte Zwecke“ erteilt werden muss. Diese Vorgabe ist Ausdruck des Zweckbindungsgrundsatzes nach Art. 5 Abs. 1 lit. b DSGVO und soll verhindern, dass die Daten des Betroffenen auf Grundlage einer Pauschaleinwilligung für Zwecke verarbeitet werden, mit denen er bei der Erteilung der Einwilligung nicht rechnen musste.

2.4.2.3 Transparenz

Möchte der Verantwortliche die Datenverarbeitung auf eine Einwilligung des Betroffenen stützen, hat er in Art. 5 Abs. 1 lit. a DSGVO verankerte Transparenzgebot zu beachten.

2.4.2.3.1 Verständlichkeit und Unterscheidbarkeit der Einwilligungserklärung

Die Einwilligungserklärung muss so gestaltet sein, dass der Betroffene erkennen kann, dass es sich um eine freiwillige Erklärung handelt, über deren Abgabe er frei entscheiden kann. Die Erklärung sollte daher bereits begrifflich als Einwilligung bezeichnet werden. Der Betroffene muss die Erklärung zudem auch ohne besondere Fachkenntnis verstehen können. Die Erklärung sollte daher kein unnötiges technisches oder fremdsprachiges Fachvokabular enthalten.[148] Daneben können auch überflüssig lange Textpassagen, versteckte Hinweise oder ungewöhnliche technische Textformate dem Transparenzgebot entgegenstehen.[149] Zur Steigerung der Verständlichkeit kann es sich anbieten, Teile der Erklärung durch Abbildungen zu visualisieren und eine an den Adressatenkreis angepasste Formulierweise zu verwenden.[150] Der Verantwortliche kann sich zur Erläuterung komplexer Sachverhalte zudem eines gestuften Informationskonzeptes im Sinne einer Mehrebenen-Datenschutzerklärung bedienen. Die Einwilligungserklärung kann dabei so gestaltet sein, dass die wesentlichen Punkte der Verarbeitung in einer überblicksartigen Erläu-

---

[146] Vgl. zu diesen Indizien *Thüsing,* BB 2016, 2165 (2166).
[147] *Thüsing,* BB 2016, 2165 (2166).
[148] *Ernst,* ZD 2017, 110 (113); *Heckmann/Paschke*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 32.
[149] *Ernst,* ZD 2017, 110 (113).
[150] So könnte etwa die unterschiedliche Intensität der Verarbeitung einzelner Daten farblich hervorgehoben werden. S. dazu mit weiteren Beispielen *Pollmann/Kipker,* DuD 2016, 378 (379 ff).

terung zusammengefasst sind und nachgelagerte Textabschnitte spezifischere Erläuterungen (z.B. zu den technischen Details) zu verschiedenen Aspekten enthalten.

Besonderheiten gelten, wenn die betroffene Person in einem einheitlichen Dokument über die Einwilligung hinausgehend noch andere Erklärungen abgibt. Bei diesen zusammengesetzten Erklärungen ist das in Art. 7 Abs. 2 S. 1 DSGVO festgelegte Trennungsprinzip zu beachten. Danach müssen die verschiedenen Erklärungen klar unterscheidbar sein. Damit unterfallen insbesondere formularmäßig vorbereitete Einwilligungserklärungen im Rahmen von allgemeinen Geschäftsbedingungen dem Anwendungsbereich von Art. 7 Abs. 2 DSGVO.[151] Abschnitte innerhalb von AGB, die sich auf das Datenschutzrecht beziehen, müssen daher besonders hervorgehoben werden.[152]

2.4.2.3.2 Informiertheit der Betroffenen

Wirksamkeitsvoraussetzung für eine Einwilligung ist zudem, dass diese in Kenntnis der Sachlage abgegeben wird. Diese Anforderung überschneidet sich mit den Informationspflichten des Verantwortlichen aus den Art. 12 ff. DSGVO.[153] Die betroffene Person muss wissen, auf welche personenbezogenen Daten sich die Einwilligung beziehen soll. Nach Erwägungsgrund 42 ist zudem über die Identität des für die Verarbeitung Verantwortlichen und über die Zwecke der Verarbeitung zu informieren.

Um eine transparente Verarbeitung auf der Grundlage einer Einwilligung sicherzustellen, muss der Verantwortliche den Betroffenen zudem informieren, dass dieser seine Einwilligung jederzeit für die Zukunft widerrufen kann (Art. 13 Abs. 2 lit. c DSGVO).

2.4.2.3.3 Rechtsfolgen bei Intransparenz

Gemäß Art. 7 Abs. 2 S. 2 DSGVO sind die Teile einer Einwilligungserklärung, die dem Trennungsprinzip nicht entsprechen, unwirksam. Die übrige Erklärung bleibt davon aber unberührt.

Im Gegensatz dazu ist die Rechtsfolge einer fehlenden Widerrufsbelehrung unklar. Das Fehlen einer Regelung über die Auswirkung eines Verstoßes gegen Art. 7 Abs. 3 S. 3 DSGVO legt nahe, dass die Wirksamkeit der Einwilligung nach dem Willen des europäischen Gesetzgebers davon unberührt bleiben soll.[154] Andererseits könnte die Überschrift von Art. 7 DSGVO – „Bedingungen für die Einwilligung“ – für einen Unwirksamkeitsautomatismus sprechen.[155] In diese Richtung zielt auch der systemati-

---

[151] *Plath*, in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 7 Rn. 5; *Stemmer* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, DSGVO Art. 7 Rn. 65; *Heckmann/Paschke*, in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 30.

[152] *Ernst* ZD 2017, 110 (113); *Schaffland/Holthaus* in: Schaffland/Wiltfang DS-GVO, Stand: 01.05.2017, Art. 7 Rn. 29; *Schulz*, in: Gola, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 41 f.; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 25.

[153] Vgl. dazu insbes. E.III.

[154] *Plath*, in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 7 Rn. 11; *Heckmann/Paschke*, in: Ehmann/Selmayr,
DS-GVO, 1. Auflage 2017, Art. 7 Rn. 41.

[155] *Plath*, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 7 Rn. 11; *Ernst*, ZD 2017, 110 (112).

sche Verweis auf Art. 13 Abs. 2 lit. c DSGVO, wonach das Bestehen eines Widerrufsrechts notwendig ist, „um eine faire und transparente Verarbeitung zu gewährleisten."[156]

Hinsichtlich der übrigen Informationspflichten aus Art. 13 DSGVO dürfte die Rechtsfolge davon abhängen, welche Angabe konkret fehlt.[157] Diese differenzierte Sichtweise lässt sich auch auf den Erwägungsgrund 42 S. 4 stützen. Danach „sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen, "um in Kenntnis der Sachlage eine Einwilligung geben zu können. Demgegenüber steht die mangelnde Kenntnis der Kontaktdaten des Datenschutzbeauftragten einer wirksamen Einwilligung nicht entgegen.[158]

2.4.2.4 Schriftformerfordernis

Nach § 26 Abs. 2 Satz 3 BDSG-neu muss der Verantwortliche die Einwilligung im Beschäftigtenkontext grundsätzlich schriftlich einholen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Das Schriftformerfordernis soll die informationelle Selbstbestimmung der betroffenen Beschäftigten absichern.[159] Besondere Umstände, die eine andere Form rechtfertigen, können sich etwa aus dem konkreten Beschäftigungsverhältnis ergeben, etwa wenn der Beschäftigte ein Home Office-Angebot nutzt und daher ganz überwiegend elektronisch mit seinem Arbeitgeber kommuniziert.[160]

2.4.3 Widerrufsrecht

Das in Art. 7 Abs. 3 S. 1 und 2 DSGVO geregelte Widerrufsrecht des Betroffenen ist ebenso wie die Einwilligung selbst Ausdruck des informationellen Selbstbestimmungsrechts. Es stellt sicher, dass eine einmalig getroffene Entscheidung zu Gunsten der Verarbeitung der eigenen Daten nicht unumkehrbar ist, selbst wenn sie freiwillig und informiert getroffen wurde. Aufgrund dieser grundrechtlichen Anknüpfung kann auf das Widerrufsrecht nicht verzichtet werden.[161] Rechtlich geschützt bleibt damit das Recht des Betroffenen, seine persönliche Einstellung in Bezug auf die Datenverarbeitung zu bestimmten Zwecken zu ändern, etwa weil die Folgen dieser Entscheidung erst nachträglich vollumfänglich erkannt werden.[162] Auf eine Begründung

---

[156] *Ernst,* ZD 2017, 110 (112); teilweise werden aber nur die Informationsbestandteile aus Art. 13 Abs. 1 DSGVO als zwingend angesehen, während die zusätzlichen Informationen nach Art. 13 Abs. 2 DSGVO nur dann notwendig sein sollen, wenn ohne sie eine faire und transparente Verarbeitung nicht gewährleistet wird, s. *Kamlah*, in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 7 Rn. 16; dagegen aber *Schmidt-Wudy* in Wolff/BrinkBeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, Art. 13 Rn. 59; *Paal* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 13 Rn. 22 f.

[157] *Schmidt-Wudy*, in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, DSGVO Art. 13 Rn. 19; *Ernst*, ZD 2017, 110 (112).

[158] *Ernst,* ZD 2017, 110 (112).

[159] *Gola*, BB 2017, 1462 (1467).

[160] *Gola*, BB 2017, 1462 (1467).

[161] *Ingold*, in: Sydow, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 46; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 35.

[162] *Frenzel* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art 7 Rn. 16; *Kühling/Buchner*, in: Kühling/Buchner, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 34.

kommt es gleichwohl nicht an, zumal der Widerruf nur mit Wirkung für die Zukunft erklärt werden kann. § 26 Abs. 2 Satz 4 BDSG-neu stellt sicher, dass der Arbeitgeber die beschäftigte Person auch über ihr Widerrufsrecht nach Art. 7 Abs. 3 DSGVO in Textform aufzuklären hat.

Nach Art. 7 Abs. 3 S. 4 DSGVO muss der Widerruf so einfach möglich sein wie die Erteilung der Einwilligung. Dem widerspricht die Vorgabe des Arbeitgebers, den Widerruf nur gegenüber einer bestimmten Einwilligung innerhalb des Unternehmens erklären zu können.[163]

Mit dem wirksamen Widerruf des Betroffenen kann die Verarbeitung seiner personenbezogenen Daten nicht länger auf die Einwilligung gestützt werden.

2.4.4 Einwilligung als Rechtsgrundlage bei adaptiven Assistenzsystemen

Als Rechtsgrundlage für den Einsatz adaptiver Assistenzsysteme wird die Einwilligung in der Praxis eine eher untergeordnete Rolle spielen. Grund hierfür sind zunächst die hohen Anforderungen, die an die Freiwilligkeit der Entscheidung zu stellen sind. Zwar beruht die Regelung in § 26 Abs. 2 BDSG-neu auf der Annahme, dass der Beschäftigte freiwillig in die Verarbeitung seiner personenbezogenen Daten durch den Arbeitgeber einwilligen kann. Mit Blick auf das faktische und rechtliche Abhängigkeitsverhältnis zwischen Beschäftigtem und Arbeitgeber darf das Risiko unfreiwillig abgegebener Einwilligung im Beschäftigtenkontext jedoch nicht unterschätzt werden. An einer echten Wahlmöglichkeit des Beschäftigten fehlt es etwa, wenn der Arbeitgeber im Zuge von Digitalisierungsmaßnahmen für einen bestimmten Arbeitsbereich den Einsatz adaptiver Assistenzsysteme vorgibt. Muss ein Beschäftigter in einer solchen Konstellation befürchten, dass er ohne Einwilligung in eine andere Abteilung versetzt wird, fehlt es an einer echten Wahlmöglichkeit. Eine dennoch abgegebene Einwilligung des Beschäftigten wäre daher unwirksam.

Aus Sicht des Arbeitgebers führt darüber hinaus die Widerrufsmöglichkeit des Betroffenen zu praktischen Hindernissen. Stützt ein Unternehmen die Einführung adaptiver Assistenzsysteme datenschutzrechtlich auf Einwilligungen der Beschäftigten, kann der Widerruf eines oder mehrerer Beschäftigten dazu führen, dass sich bereits getätigte Investitionen in die Entwicklung und die Anschaffung eines Systems mit einem Mal als nutzlos erweisen. Die damit verbundenen wirtschaftlichen Risiken wird ein Arbeitgeber nur selten in Kauf nehmen können. Etwas anderes kann in Situationen anzunehmen sein, in dem ein adaptives Assistenzsystem im Unternehmen unter Einbeziehung einzelner interessierter Beschäftigter entwickelt oder getestet werden soll. In einer solchen Situation kann es ein gangbarer Weg sein, sich für die Datenverarbeitung während der Entwicklungs- bzw. Testphase auf eine Einwilligung der beteiligten Beschäftigten zu stützen.

---

[163] Vgl. *Frenzel* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 7 Rn. 17.

2.5 Rechtsgrundlage für die Verarbeitung von Daten Dritter

Bei der Anwendung adaptiver Assistenzsysteme kann es auch zur Erhebung und anschließenden Nutzung von Daten Dritter kommen, welche nicht Beschäftigte des Unternehmens sind, welches die Assistenzsysteme einsetzt. Die Datenerfassung kann dabei zufällig erfolgen, bspw. wenn ein Besucher durch das Bild einer Kamera läuft. Die Datenerfassung kann aber auch zielgerichtet erfolgen. Dies ist bspw. der Fall bei externen Monteuren, die zu Reparaturzwecken die Systeme warten, oder bei Besuchern, denen die Assistenzsysteme vorgeführt werden. Eine weitere Fallgruppe betrifft adaptive Assistenzsysteme, die gezielt Daten Dritter zur Aufgabenbewältigung benötigen. Das sind bspw. Systeme, die mit Kunden- oder Lieferantendaten arbeiten.

In diesen Fällen greifen die Grundlagen zum Beschäftigtendatenschutz nicht.

2.5.1 Verarbeitung im Rahmen der Erfüllung von Verträgen

Bei Betroffenen, die mit dem Arbeitgeber in einem Vertragsverhältnis stehen, kommt als Rechtfertigung für die Datenverarbeitung Art. 6 Abs. 1 b) DSGVO in Betracht. Danach ist die Verarbeitung rechtmäßig, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Diese Rechtfertigung greift dann, wenn ein Vertragsverhältnis mit der betroffenen Person besteht, wenn also Kunde oder Lieferant auch derjenige ist, dessen Daten verarbeitet werden sollen. Ist Kunde oder Lieferant demgegenüber ein Unternehmen und wird eine Person beispielsweise als Ansprechpartnerin genannt, kann die Verarbeitung nicht auf Art. 6 Abs. 1 b) gestützt werden.

Weiterhin muss die Datenverarbeitung zur Erfüllung des Vertrags erforderlich sein. Die Datenverarbeitung muss damit in einem konkreten Zusammenhang zur vertraglichen Leistungspflicht stehen. So ist die Anschrift eines Kunden erforderlich zur Versendung des bestellten Produkts. Sollen jedoch Kundendaten zur Feststellung von Profilen oder Präferenzen verarbeitet werden, fällt diese Verarbeitung nicht unter das zur Vertragsdurchführung Erforderliche.

Ein Anwendungsbeispiel wäre ein Assistenzsystem wie z.B. eine Datenbrille, die dem Beschäftigten unmittelbar die Kundenbestellung anzeigt und ihm gleichzeitig einen Kommissionierungsauftrag erteilt, wo und wann er die bestellte Ware aufzunehmen hat. Die Datenverarbeitung erfolgt zwar hier im Rahmen der internen Organisation, allerdings ist der Zusammenhang zur Bestellung gegeben, so dass dieser Verarbeitungsschritt von der Vertragserfüllung gedeckt ist.

2.5.2 Einwilligung des Dritten

Als Rechtfertigung kommt ebenfalls die Einwilligung des Betroffenen in Betracht. Zu denken wäre an einen Besucher, dem das Assistenzsystem mit „Echtdaten“ vorgeführt wird. Die Einwilligung kann auch in der Beziehung zu Kunden oder Lieferanten eine Rolle spielen, wenn die Datenverarbeitung nicht zur Vertragserfüllung erforderlich ist. Zu denken wäre beispielsweise daran, dass der Kunde oder Lieferant, oder auch deren Beschäftigte, zustimmen, dass ihre Daten bei der Anwendung adaptiver Assistenzsysteme genutzt werden. So könnten bspw. Kunden- oder Lieferantenpräferenzen, Bestellperioden oder sonstige Merkmale durch lernfähige Systeme analysiert und Profile erstellt werden.

Voraussetzung für die Einwilligung ist, dass diese informiert erfolgt, d.h. der Betroffene vorab über die geplante Datenverarbeitung aufgeklärt wurde.[164] Die Einwilligung muss zudem für einen konkret bestimmten Zweck eingeholt werden und sie muss freiwillig erfolgen.[165] Auch hier kann der Betroffene seine Einwilligung für die Zukunft widerrufen.

2.5.3 Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO

Bei der Verarbeitung von Daten Dritter im Zusammenhang mit adaptiven Assistenzsystemen wird die Interessenabwägung die wichtigste Rechtfertigungsgrundlage darstellen. Auch hier sind – ähnlich wie bei der Verarbeitung von Beschäftigtendaten außerhalb des Beschäftigtenkontextes – die jeweiligen Interessen des Betroffenen und des Verarbeiters gegenüberzustellen. Abhängig von der Intensität des Eingriffs ist dem Betroffenen eine Verarbeitung seiner Daten zuzumuten, wenn legitime Interessen des Unternehmers eine solche Datenverarbeitung erforderlich machen. Wesentlicher Gesichtspunkt dürfte in diesem Zusammenhang die Transparenz der Verarbeitung sein. Wird am Eingang der Fabrikhalle darauf aufmerksam gemacht, dass Videoaufzeichnungen erfolgen, muss der Besucher damit rechnen, dass das Betreten aufgezeichnet wird. Je nach Zweck der Videoaufzeichnung muss der Besucher diese Aufzeichnung dann hinnehmen. Entsprechende Hinweise können auch für Besucher, Monteure oder sonstige Betroffene erfolgen, und damit die Abwägung zugunsten des verantwortlichen Unternehmers beeinflussen.

---

[164] Vgl. oben D.IV.2.2.
[165] Vgl. oben D.IV.2.

3 Betroffenenrechte des Beschäftigten und damit korrespondierende Pflichten des Arbeitgebers

3.1 Überblick Betroffenenrechte nach der DSGVO

Im III. Kapitel der DSGVO sind eine Vielzahl sog. Betroffenenrechte geregelt, die dem Beschäftigten, dessen Daten verarbeitet werden, bestimmte Rechte im Hinblick auf den Umgang mit seinen Daten einräumen. Damit korrespondieren Pflichten des oder der Verantwortlichen. Zu den Betroffenenrechten gehören das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Löschung (Art. 17 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie das neue Recht auf Datenübertragbarkeit oder -portabilität (Art. 20 DSGVO).

Da die Ausübung der Betroffenenrechte stets Kenntnis von der Datenverarbeitung voraussetzt, finden sich in Art. 12 DSGVO zunächst allgemeine Bestimmungen zur Transparenz und den Modalitäten der Ausübung der Betroffenenrechte, sodann im zweiten Abschnitt (Art. 13-15 DSGVO) die konkreten Informationspflichten. Art. 13 und 14 DSGVO übernehmen die bereits dem BDSG-alt zugrundeliegende Unterscheidung zwischen Informationspflichten bei Direkterhebung[166] und bei der sog. Dritterhebung, d.h. in Fällen, in denen personenbezogene Daten nicht bei der betroffenen Person erhoben werden.[167]

Verstöße gegen die Betroffenenrechte werden gem. Art. 83 Abs. 5 lit. b DSGVO sanktioniert. Gerade weil die Stärkung der Betroffenenrechte ein Hauptanliegen der DSGVO ist, muss damit gerechnet werden, dass die Aufsichtsbehörden Verstöße in diesem Bereich vermehrt sanktionieren werden.

3.2 Modalitäten

Die allgemeinen Modalitäten zur Ausübung der Betroffenenrechte sowie die von dem Verantwortlichen zwingend zu beachtenden Anforderungen finden sich in Art. 12 Abs. 1 bis 6 DSGVO.

3.2.1 Adressat

Die Betroffenenrechte gelten nur gegenüber dem Verantwortlichen. Dies ist gem. Art. 4 Nr. 7 DSGVO

„die natürliche oder juristische Person, die Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; (...)“

---

[166] ehem. § 4 Abs. 3 BDSG-alt, nun Art. 13 DSGVO.

[167] ehem. § 33 BDSG-alt, nun Art. 14 DSGVO; jedoch gilt der Grundsatz der Direkterhebung unter der DSGVO nicht mehr.

Bei adaptiven Arbeitsassistenzsystemen stellt sich die Frage, wer Verantwortlicher im Sinne dieser Definition ist. Maßgebliches Kriterium dabei ist die faktische Entscheidungsmacht. Handelt es sich um „einfache“ Anwendungen wie RFID-Tags und werden diese vom Arbeitgeber selbst gestaltet bzw. herausgegeben, ist die Einordnung noch relativ klar. Der Arbeitgeber setzt diese Anwendungen ein und entscheidet über Auswertung und Verwendung der so erhobenen Daten.

Schwieriger wird es bereits mit Blick auf komplexere Anwendungen, wie etwa Datenbrillen oder „intelligente“ Handschuhe, bei denen regelmäßig Herstellung, Ausgabe des Systems und ggf. weitere Datenverarbeitungen von verschiedenen Personen durchgeführt werden, die nicht dem Unternehmen angehören müssen.

Die ursprüngliche Verantwortlichkeit liegt in der Entwicklung des Assistenzsystems. Denn wer aus eigenem wirtschaftlichem Interesse bestimmte Assistenzsysteme in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt die Mitverantwortlichkeit für die Rechtmäßigkeit solcher Angebote.[168] Der Entwickler gibt den technisch-organisatorischen Rahmen der Assistenzsysteme vor und hat die Möglichkeit, unter Berücksichtigung des Grundsatzes der Datensparsamkeit in Gestalt des Datenschutzes durch Technikgestaltung („Privacy by design“) die Datenverarbeitung zu regeln.[169] Dieser verfügt damit über maßgebliche Entscheidungskompetenzen im Sinne der vorstehenden Definition.[170]

Gleichzeitig schafft aber der Arbeitgeber in Ausübung seines Direktionsrechts durch das Bereitstellen eine wesentliche Voraussetzung für die Verarbeitung.[171] Damit ist der Arbeitgeber gleichzeitig Verantwortlicher aufgrund seiner Zuständigkeit in Bezug auf die Daten seiner Beschäftigten.[172] Dies gilt ungeachtet seiner faktischen Möglichkeiten zur Beeinflussung des Systems. Insofern wird man mit zunehmender Komplexität des eingesetzten Systems grundsätzlich in den Bereich der gemeinsamen Verantwortlichkeit zwischen Hersteller und Arbeitgeber rücken.[173]

Bei gemeinsamer Verantwortlichkeit ergibt sich grundsätzlich ein Pflichtengleichlauf der Verantwortlichen, der sich schließlich auch in einer gesamtschuldnerischen Haftung für Pflichtverletzungen äußert. Art. 26 Abs. 1 DSGVO sieht für den Fall der gemeinsamen Verantwortlichkeit vor, dass diese durch Vereinbarung festlegen, wer

---

[168] So auch die deutschen Aufsichtsbehörden bei der Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, 6./7. April 2016 zu Wearables und Gesundheits-Apps- Sensible Gesundheitsdaten effektiv schützen!; ebenso die Art. 29-Datenschutzgruppe, WP 223 (Opinion 8/14) vom 16.09.2014, S. 21.

[169] vgl. Blinn DSRITB 2016, 519.

[170] vgl. Artikel-29-Datenschutzgruppe, Opinion 8/2014 on the Recent Developments on the Internet of Things, 14/EN/WP 223, S. 11.

[171] *Weichert*, NZA 2017, 565 (566), Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten.

[172] vgl. zur Verantwortung aufgrund implizierter Zuständigkeit: Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und Auftragsverarbeiter“, 00264/10/DE WP 169, S. 13.

[173] vgl. *Weichert*, NZA 2017, 565 (569), Die Verarbeitung von Wearable-Sensordaten bei Beschäftigten; a.A. *Blinn* DSRITB 2016, 519 (526). Mit einer Parallelfrage befasst sich derzeit der EuGH, vgl. den Vorlagebeschluss des BVerwG vom 25.2.2016 - 1 C 28.14 (OVG Schleswig, VG Schleswig), ZD 2016, 393 – Facebook-Fanpage.

konkret welche Verpflichtungen übernimmt. Dennoch kann der Betroffene sich jederzeit an jeden Verantwortlichen wenden.

Geht man davon aus, dass in Bezug auf komplexe adaptive Assistenzsysteme eine gemeinsame Verantwortlichkeit vorliegt, kommt einer klaren Verantwortungszuweisung, wie sie Art. 26 DSGVO vorschreibt, eine hohe Bedeutung zu. Auch eine Vereinbarung darüber, wer Anlaufstelle für die Beschäftigten bei der Ausübung ihrer Betroffenenrechte und wer verpflichtet ist, die Informationspflichten einzuhalten, wäre dabei denkbar. Jedoch ist im speziellen Kontext des Beschäftigtendatenschutzes zu bedenken, dass sich die Beschäftigten zur Wahrnehmung ihrer Betroffenenrechte vornehmlich an den Arbeitgeber wenden werden und dies auch dürfen. Das beeinflusst zwar nicht das Innenverhältnis, insb. auch nicht die haftungsrechtlichen Betrachtung[174] und mag zudem die tatsächlichen Gegebenheiten nicht stets widerspiegeln, ist aber mit Blick auf die sich aus dem Arbeitsverhältnis ergebenden Fürsorgepflichten geboten.[175] Damit wäre es unzulässig, wenn sich der Arbeitgeber im Wege einer Vereinbarung mit dem Hersteller seiner dahingehenden Verantwortung entledigen wollte.

Wird ein externer Dienstleister mit einer weiteren Verarbeitung beauftragt, kommt, abhängig von der konkreten Ausgestaltung der Kontrollbefugnisse,[176] sowohl eine Auftragsverarbeitung (Art. 28 DSGVO) als auch eine (weitere) gemeinsame Verantwortlichkeit in Betracht. Da die Betroffenenrechte nur gegenüber dem Verantwortlichen geltend gemacht werden können, beeinflusst eine solche Konstellation lediglich die zu treffenden Regeln im Innenverhältnis, bliebe für den Beschäftigten aber faktisch ohne Konsequenz.

An die Grenzen möglicher Zuordnung anhand der DSGVO stößt man beim Einsatz autonom handelnder, intelligenter Systeme, d.h. bei solchen, die in einem gewissen Umfang intelligentes Verhalten aufweisen, zielorientiert handeln und über ein gewisses Maß an Lernfähigkeit verfügen.[177] Dabei werden unter Verwendung der oben angesprochenen Anwendungen (RFID Technologie, Wearables oder auch Kamerasysteme) personenbezogene Daten erfasst und anschließend selbstlernend und autonom agierend mit anderen Systemen kommuniziert und in Echtzeit Entscheidungen gefällt.[178] Die Zwecke und Mittel der Datenverarbeitung werden dabei dezentral angesteuert, sind aber das Ergebnis vielfacher Interaktion und Koordination zwischen vollständig oder teilweise autonom handelnden Systemen. Entscheidungen über die Zwecke der Verarbeitung werden hier autonom vom „System“ getroffen.[179]

---

[174] S. zur gesamtschuldnerischen Haftung bei gemeinsamer Verantwortlichkeit Art. 82 Abs. 2 DSGVO.

[175] S. dazu auch die in EG 79 DSGVO zum Ausdruck kommende generelle Zielrichtung, die Verantwortung klar zuzuordnen.

[176] vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und Auftragsverarbeiter“, 00264/10/DE WP 169, S.18.

[177] Insgesamt dazu *Kirn/Müller-Hengstenberg*, MMR 2014, 225 (ff.), Intelligente (Software-)Agenten: Von der Automatisierung zur Autonomie? Verselbstständigung technischer Systeme.

[178] S. näher dazu Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 15.

[179] *Geisberger*/*Broy* (Hrsg.), agendaCPS, Integrierte Forschungsagenda Cyber-Physical Systems, acatech Studie, 2012, S. 64 ff; *Hansen*/*Thiel*, DuD 2012, 26 (28), Cyber-Physical Systems und Privatsphärenschutz.

In diesem Fall stellt die Zuordnung zu einer „natürlichen oder juristische Person, Behörde, Einrichtung oder anderen Stelle“ (s. Art. 4 Nr. 7 DSGVO) ein Problem dar.

Nach derzeitigem Diskussionsstand, der sich vor allem auf den Bereich des autonomen Fahrens konzentriert, wird versucht, die Zuordnung über Parallelen zum Haftungsrecht vorzunehmen. Die Vorschläge, Robotern bzw. künstlicher Intelligenz eine eigene beschränkte Rechtssubjektivität zuzusprechen, überzeugen aus rechtlicher Sicht nicht. In Ermangelung einer klaren Zuordnung, wie der Halterhaftung für den Bereich des autonomen Fahrens, überzeugen in diesem Zusammenhang am ehesten die Vornahme der Zurechnungen der Vertreterhaftungen aus §§ 278 BGB, § 831 BGB.[180] Im Ergebnis wird man auch bei derartigen Systemen den Arbeitgeber als datenschutzrechtlichen Verantwortlichen betrachten müssen.

3.2.2 Berechtigter

Der Verantwortliche ist nur der betroffenen Person gegenüber zur Information und zum Tätigwerden verpflichtet (Art. 12 Abs. 1 DSGVO). Im Beschäftigtenkontext sind dies die von der Datenverarbeitung betroffenen Beschäftigten.

3.2.3 Form

Nach Art. 12 Abs. 1 DSGVO muss der Arbeitgeber den Beschäftigten zunächst über die Verarbeitung seiner personenbezogenen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache informieren. Im Zusammenhang mit den hier thematisierten adaptiven Arbeitsassistenzsystemen stellt bereits das Erfordernis, die Informationen präzise und insb. auch leicht verständlich zur Verfügung zu stellen, eine große Herausforderung dar. Dabei gilt es den Grundsatz zu beachten, dass je umfangreicher und komplexer die Datenverarbeitung ist, desto stärker dies durch ein hohes Maß an Transparenz gegenüber der betroffenen Person zu kompensieren ist.[181]

Die Übermittlung der Information kann schriftlich oder „in anderer Form“ erfolgen (Art. 12 Abs. 1 S. 2 DSGVO). So können die Informationen ausweislich des Art. 12 Abs. 7 DSGVO auch in Kombination mit standardisierten Bildsymbolen (sog. Icons) bereitgestellt werden, welche gem. Art. 12 Abs. 8 DSGVO von der Kommission im Wege eines delegierten Rechtsaktes (Art. 92 DSGVO) festgelegt werden sollen. Hinsichtlich der anderen Formen der Bereitstellung führt EG 58 DSGVO aus, dass die Informationen auch in elektronischer Form, beispielsweise auf einer Website bereitgehalten werden können, wenn sie für die Öffentlichkeit bestimmt ist.[182] Hieraus lässt sich mit Blick auf Transparenz- und Effizienzgesichtspunkte insgesamt schließen, dass sich der Gesetzgeber technologischen Entwicklungen gegenüber öffnen wollte. Insbesondere in Situationen, in denen es wegen der großen Zahl der Beteiligten und der Komplexität der dazu benötigten Technik für die betroffene Person schwer ist zu erkennen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene

---

[180] S. insgesamt dazu *Spindler*, CR 2015, 766 (ff., insb. 775), Roboter, Automation, künstliche Intelligenz, selbst-steuernde KfZ – Braucht das Recht neue Haftungskategorien?

[181] vgl. bezogen auf Smart Meter Datenschutz: *Keppeler*, EnWZ 2016, 99 (99) Personenbezug und Transparenz im Smart Meter-Datenschutz zwischen europäischem und nationalem Recht.

[182] Falls von dem Betroffenen verlangt, kann die Information aber auch mündlich erfolgen, wobei in diesem Fall darauf zu achten ist, dieses Vorgehen hinreichend zu dokumentieren.

Daten verarbeitet werden, sollte diese Möglichkeit zur Anwendung kommen. Als Beispiel hierfür wird die Werbung im Internet genannt, das sog. „behavioral targeting“, bei dem eine Vielzahl von Akteuren mit für die betroffene Person nur schwer nachvollziehbaren tracking-Methoden personenbezogene Daten verarbeiten, um sie gezielt werblich ansprechen zu können. In ähnlicher Weise stellt sich die Datenverarbeitung beim Einsatz adaptiver Arbeitsassistenzsysteme dar. Auch hier können beispielsweise über eine Vielzahl von Sensoren personenbezogene Daten erhoben werden, die dann von einem System zusammengeführt und zur Grundlage von Entscheidungen, etwa zu darauffolgenden Arbeitsschritten und den dafür bestgeeigneten Beschäftigten gemacht werden.[183]

Aus Unternehmenssicht dürfte im Rahmen von Betriebsvereinbarungen auch eine kollektive Information des Betriebsrats als „Informationsmediär“ für die Beschäftigten in Betracht kommen.[184] Damit würden dann auch die einzelnen Beschäftigten als informiert gelten.

Die Geltendmachung der Rechte aus Art. 15ff. DSGVO unterliegt keinen besonderen Formerfordernissen. Der Verantwortliche ist gem. Art. 12 Abs. 2 DSGVO jedoch verpflichtet, dem Beschäftigten die Ausübung der Rechte aus Art. 15 bis 22 DSGVO zu erleichtern, etwa indem Anträge auf elektronischem Wege gestellt werden können.[185] Es bleibt aber grundsätzlich dem Verantwortlichen überlassen, ob und auf welche Weise er die Geltendmachung der Betroffenenrechte (etwa Auskunftsanträge vom Beschäftigten) kanalisiert; so kann der Verantwortliche z.B. auf seinem Internetauftritt ein Formular für Auskunftsanfragen bereithalten.[186] Alternativ wird vorgeschlagen, eine eigene E-Mailadresse (etwa: auskunftsverlangen@...) einzurichten.[187] Vertretbar erscheint es aber auch, eine allgemeine info@... – Adresse vorzusehen, solange deutlich gemacht wird (etwa durch einen kurzen Erläuterungstext), dass hierüber auch die Betroffenenrechte nach der DSGVO geltend gemacht werden können.

3.2.4 Fristen

3.2.4.1 Fristen in Bezug auf die Informationspflichten

Werden die Daten direkt bei der betroffenen Person erhoben, statuiert Art. 13 Abs. 1 DSGVO, dass die Informationspflichten zum Zeitpunkt der Erhebung erfüllt sein müssen. Werden die Daten nicht direkt beim Betroffenen erhoben, regelt Art. 14 Abs. 3 DSGVO nähere Anforderungen an die Fristen: Art. 14 Abs. 3 lit. a DSGVO stellt auf den Zeitpunkt der Erlangung ab und fordert, den Betroffenen unter Berücksichtigung der Umstände des Einzelfalles innerhalb einer angemessenen Frist über die Erhebung zu informieren. Diese Frist darf maximal einen Monat betragen. Sollen die Daten zur Kommunikation mit dem Betroffenen verwendet werden, müssen die Informa-

---

[183] Vgl. Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 15.

[184] *Wybitul*, ZD 2016, 203 (208), Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte?; *Riesenhuber* in: Wolff/Brink, BeckOK Datenschutzrecht, 19. Edition, Stand: 01.02.2017, Art. 88 DSGVO, Rn 87.

[185] S. dazu EG 59 DSGVO.

[186] *Schmidt-Wudy* in Wolff/Brink, BeckOK Datenschutzrecht, 18. Edition, Stand: 01.11.2016, Art. 15 DSGVO, Rn. 46.

[187] *Schmidt-Wudy*, in Wolff/Brink, BeckOKDatenschutzrecht, 18. Edition, Stand: 01.11.2016, Art. 15 DSGVO, Rn. 46.

tionspflichten spätestens zum Zeitpunkt der ersten Kontaktaufnahme erfüllt sein. Für den Fall der Offenlegung an einen anderen Empfänger gilt der Zeitpunkt der erstmaligen Offenlegung.

3.2.4.2 Antragsbezogene Fristen

Auch wenn der Beschäftigte von seinen Betroffenenrechten Gebrauch macht und einen Antrag bspw. auf Auskunft oder Löschung stellt, gelten feste Reaktionsfristen.

Der Verantwortliche muss gem. Art. 12 Abs. 3 Satz 1 DSGVO unverzüglich, spätestens aber innerhalb eines Monats nach Geltendmachung der Betroffenenrechte aus Art. 15 bis 22 tätig werden. Diese Frist kann um bis zu drei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. In jedem Fall wäre aber auch dann eine Unterrichtung darüber im Rahmen der Ein-Monats-Frist geboten. Will oder kann der Verantwortliche dem Ersuchen nicht nachkommen, hat er dies der betroffenen Person ohne Verzögerung mitzuteilen (Art. 12 Abs. 4 DSGVO). Lehnt der Verantwortliche einen Antrag der betroffenen Person nach Art. 15 ff. DSGVO ab, ist er gem. Art. 12 Abs. 4 DSGVO verpflichtet, die betroffene Person über die Gründe zu unterrichten und sie auf die Möglichkeit zur Beschwerde bei der Aufsichtsbehörde nach Art. 77 Abs. 1 DSGVO oder einen gerichtlichen Rechtsbehelf (Art. 79 DSGVO) hinzuweisen.[188]

3.2.5 Unentgeltlichkeit

Der Verantwortliche ist gem. Art. 12 Abs. 5 Satz 1 DSGVO verpflichtet, die Informationen sowie alle Mitteilungen und Maßnahmen nach den Art. 15 bis 22 und 34 DSGVO unentgeltlich zur Verfügung zu stellen. Lediglich in Fällen missbräuchlicher Anträge kann der Verantwortliche gem. Art. 12 Abs. 5 Satz 2 lit. a DSGVO unter Berücksichtigung der Verwaltungskosten für die Bearbeitung des jeweiligen Antrags ein angemessenes Entgelt für sein Tätigwerden verlangen oder gem. Art. 12 Abs. 5 Satz 2 lit. b DSGVO ein Tätigwerden verweigern. Der Verantwortliche hat hier ein Wahlrecht. Die Höhe des angemessenen Entgelts ist – anders als noch in der Datenschutzrichtlinie – von der tatsächlichen Höhe der dem Verantwortlichen entstehenden Kosten entkoppelt, eine Pauschalisierung ist zulässig. Ein streng kostenbasierter Ansatz ist also nicht erforderlich. In der bisherigen Kommentarliteratur wird aber empfohlen, in etwa den Durchschnitt der tatsächlichen Verwaltungskosten zu veran-

---

[188] Für eine solche Rechtsbehelfsbelehrung bietet sich ein Textbaustein an, der sich eng am Gesetzeswortlaut orientiert, etwa wie folgt: „Wenn Sie der Ansicht sind, dass wir Ihren Antrag zu Unrecht abgelehnt haben, so haben Sie das Recht auf Beschwerde hiergegen bei einer Datenschutzaufsichtsbehörde, insbesondere in dem Mitgliedstaat Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes gegen die Datenschutz-Grundverordnung (Art. 77 Abs. 1 Datenschutz-Grundverordnung). Weiterhin haben Sie das Recht auf einen wirksamen gerichtlichen Rechtsbehelf (Art. 79 Abs. 1 Datenschutz-Grundverordnung). Für Klagen gegen einen anderen Verantwortlichen oder gegen einen Auftragsverarbeiter sind die Gerichte des Mitgliedstaats zuständig, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat. Wahlweise können solche Klagen auch bei den Gerichten des Mitgliedstaats erhoben werden, in dem Sie ihren Aufenthaltsort haben (vgl. Art. 79 Abs. 2 Datenschutz-Grundverordnung).“

schlagen.[189] Der Verantwortliche ist beweisbelastet, dass der Antrag offenkundig unbegründet oder exzessiv ist.

3.3 Transparenz der Verarbeitung

Beim Einsatz adaptiver Arbeitsassistenzsysteme werden vielfältige Daten kontextsensitiv, tätigkeitsbegleitend und individuell zuordenbar erhoben und ausgewertet. Dabei fallen auch „kritische Parameter“ an, welche Rückschlüsse des Arbeitgebers auf Leistung, Verhalten, Fehler, Arbeitszeit und Anwesenheit, aber auch auf die Gesundheit der Beschäftigten zulassen können. Dieser Umstand, die Zwecke und Verwendungen der personenbeziehbaren Daten sind unter Umständen nicht für alle Beteiligten transparent. Demgegenüber ist eines der wesentlichen Anliegen der DSGVO, durch gesteigerte Informations- und Mitteilungspflichten die Datenverarbeitung für die Betroffenen deutlich transparenter zu machen.

Dass dem Transparenzgrundsatz auch bei der Datenverarbeitung im Beschäftigtenkontext besondere Bedeutung zukommt, verdeutlichen Art. 88 Abs. 2 DSGVO i.V.m. § 26 Abs. 5 BDSG-neu. Nach Art. 88 Abs. 2 DSGVO sind die Mitgliedstaaten zu angemessenen und besonderen Maßnahmen im Hinblick auf die Transparenz der Verarbeitung verpflichtet. Dieser Verpflichtung ist der deutsche Gesetzgeber mit § 26 Abs. 5 BDSG-neu nachgekommen, wonach der Verantwortliche geeignete Maßnahmen ergreifen muss, um sicherzustellen, dass die in Art. 5 DSGVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Der Beschäftigte muss also klar erkennen und nachvollziehen können, ob, von wem und zu welchem Zweck seine personenbezogenen Daten verarbeitet werden[190]. Nicht offen erkennbare Überwachungsvorgänge (wie etwa eine heimliche Videoüberwachung oder ähnliche verdeckte Überwachungen am Arbeitsplatz) sind damit grundsätzlich nicht zu vereinbaren, es sei denn, eine solche Maßnahme kann auf eine ausdrückliche Ausnahmevorschrift gestützt werden. Eine Ausnahme kann gem. § 33 Abs. 1 Nr. 2 lit. a BDSG-neu insbesondere dann angenommen werden, wenn eine Interessenabwägung ergibt, dass durch die Informationserteilung erhebliche Geschäftszwecke des Arbeitgebers gefährdet wären.[191]

Verstöße gegen das Transparenzgebot und dessen Ausgestaltung in Art. 12ff. DSGVO können mit empfindlichen Geldbußen von bis zu 20 000 000 EUR oder von bis zu 4% des gesamten weltweiten Jahresumsatzes eines Unternehmens geahndet werden, vgl. Art. 83 Abs. 5 lit. a und lit. b DSGVO. Auch vor diesem Hintergrund ist es erforderlich, die sich konkret aus der DSGVO ergebenden Anforderungen an die Transparenz der Datenverarbeitung näher zu hinterfragen.

3.3.1 Exkurs: Informationspflicht § 81 BetrVg

Wenn auch nicht aus datenschutzrechtlicher Sicht, so ist doch im Zusammenhang mit dem Einsatz adaptiver Arbeitsassistenzsysteme § 81 BetrVG zu berücksichtigen. Danach ist der Arbeitgeber konkret dazu verpflichtet, den Beschäftigten über die ihn

---

[189] *Paal* in Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 12 Rn. 68.
[190] vgl. EG 58 DSGVO.
[191] *Gola*/*Thüsing*/*Schmidt*, DuD 2017, 248, Was wird aus dem Beschäftigtendatenschutz?

betreffenden Arbeitsbedingungen zu informieren. Von besonderer Bedeutung im Zusammenhang mit adaptiven Assistenzsystemen ist Abs. 4, der eine Pflicht des Arbeitgebers normiert, den Beschäftigten über die aufgrund einer Planung von technischen Anlagen, Arbeitsverfahren und Arbeitsabläufen vorgesehenen Maßnahmen und deren Auswirkungen auf seinen Arbeitsplatz und die Arbeitsumgebung zu unterrichten. Diese Vorgaben sind also bei Neueinführung technischer Systeme zu berücksichtigen.

3.3.2 Informationspflichten nach der DSGVO

Nähere Konkretisierung erfährt der Transparenzgrundsatz in Art. 12 ff. DSGVO. Der Katalog der zu erteilenden (Vorab-)Informationen (Art. 13, Art. 14 DSGVO), die dem Betroffenen zur Verfügung gestellt werden müssen, wurde gegenüber den Anforderungen des BDSG-alt erheblich ausgeweitet.

3.3.2.1 Umfang der Informationspflichten in Abhängigkeit von der Erhebung

Die in Art. 13 und 14 DSGVO vorgenommene Unterscheidung zwischen Direkt- und Dritterhebung ist kein neues Phänomen unter der DSGVO. Vielmehr galt diese Unterscheidung bereits unter der Datenschutzrichtlinie[192]. Daran anknüpfend ergeben sich unterschiedlich weitreichende Informationspflichten.

3.3.2.2 Abgrenzungsmaßstab Direkt- und Dritterhebung

Fraglich ist, wann nach der DSGVO eine Direkterhebung und wann eine Erhebung aus anderen Quellen anzunehmen ist. Eine eindeutige Definition hierfür findet sich in der DSGVO selbst nicht. Aus EG 39 der Datenschutzrichtlinie ergab sich jedoch, dass eine Direkterhebung dann anzunehmen ist, wenn die Daten unmittelbar bei der betroffenen Person erhoben werden. Dies wird überwiegend dann angenommen, wenn die betroffene Person Kenntnis von der Datenerhebung hat und/oder an der Erhebung mitwirkt.[193]

Gegenüber dieser auf die betroffene Person abstellende Betrachtung vertritt Bäcker[194] die Ansicht, dass auf den Verantwortlichen und dessen Möglichkeit, mit der betroffenen Person in Kontakt zu treten, abzustellen sei. Anders ließe sich die Anforderung aus Art. 13 Abs. 1 und 2 DSGVO, die Informationen im Zeitpunkt der Datenerhebung zu erteilen, nicht umsetzen. Danach sei etwa die Videoüberwachung im öffentlichen Raum ebenso ein Fall der Direkterhebung wie die heimliche Observation

---

[192] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

[193] *Franck* in: Gola, DS-GVO, 1. Auflage 2017, Art. 13 Rn. 4; *Schmidt-Wudy* in: Wolff/Brink, BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, Art. 14 DSGVO, Rn. 31; *Scholz/Sokol* in: *Simitis*, Bundesdatenschutzgesetz, 8. Auflage 2014, § 4 Rn. 20; *Brühann* in: Grabitz/Hilf, Das Recht der Europäischen Union, 40. Auflage 2009, Art. 10 Richtlinie 95/46/EG, Rn. 7; *Gola*/*Pötters*/*Wronka*, Handbuch Arbeitnehmerdatenschutz, 7. Auflage 2016, Rn. 1454a.

[194] *Bäcker* in: Kühling/Buchner, Datenschutzgrundverordnung, 1. Auflage 2017, Art. 13 Rn. 13.

durch einen Privatdetektiv. Lediglich wenn die Daten aus öffentlichen Quellen oder bei Dritten erhoben werden, sei Art. 14 DSGVO einschlägig.[195]

Dieser Ansicht ist nicht zuzustimmen. Bäcker verkennt Sinn und Zweck des Transparenzgrundsatzes: Die Informationspflichten dienen als Vorfeldmaßnahme der effektiven Rechtewahrnehmung der betroffenen Person. Nur wer weiß, dass und wie personenbezogene Daten erhoben werden, kann seine Rechte aus Art. 15-22 DSGVO entsprechend wahrnehmen.

Damit betrifft Art. 13 DSGVO in Abgrenzung zu Art. 14 DSGVO sowohl Fälle, in denen Daten aktiv von der betroffenen Person zur Verfügung gestellt werden, wie etwa bei der Eingabe personenbezogener Daten in eine Onlinemaske, als auch Fälle, in denen die betroffene Person eine Datenerhebung bewusst duldet, wie in Fällen offener (transparenter) Videoüberwachung.

3.3.2.3 Abgrenzungsfragen im Zusammenhang mit adaptiven Arbeitsassistenzsystemen

Beim Einsatz adaptiver Arbeitsassistenzsysteme kommen neben aktiven Eingaben regelmäßig auch Datenverarbeitungsvorgänge zur Anwendung, die ohne Mitwirkung und Kenntnis des Betroffenen erfolgen. Aufgrund der hohen Komplexität und der Fülle der Datenverarbeitungsvorgänge haben Beschäftigte regelmäßig keine Kenntnis der genutzten personenbezogenen Daten und der Zwecke der Verarbeitung. Prozessrelevante Informationen werden in Echtzeit an die aktuelle Situation des Beschäftigten angepasst. Hierfür werden während der Nutzung des Systems ständig Daten über die räumliche Umgebung, Aufgabe, Nutzer etc. erhoben und verarbeitet. Grundlage hierfür bilden Sensoren die am Körper getragen und/oder im Arbeitsumfeld angebracht werden.[196] Die Informationsgenerierung erfolgt zudem im Hintergrund ohne ein weiteres Zutun des Beschäftigten, also ohne dass dieser die Informationen aktiv anfordern müsste. Kontextsensitive Arbeitsassistenzsysteme arbeiten dann autonom, d.h. ohne den bewussten manuellen Eingriff des Nutzers.[197] Zweck des Einsatzes adaptiver Arbeitsassistenzsysteme ist es also insbesondere im Hintergrund zu agieren und damit den Beschäftigten bei seinen Aufgaben zu unterstützen.[198] Daher wird man bei derartigen adaptiven Assistenzsystemen regelmäßig von einer Dritterhebung ausgehen müssen.

Daneben werden aber auch weitere Verfahren der Datenerfassung wie Identifikationssysteme eingesetzt. In diesen Fällen werden die Daten vom Beschäftigten selbst

---

[195] *Bäcker* in: Kühling/Buchner, Datenschutzgrundverordnung, 1. Auflage 2017, Art. 13 Rn. 13ff.

[196] vgl. hierzu insgesamt Forschungsbericht Digitalisierung und Beschäftigtendatenschutz, S. 8ff.

[197] vgl. zu den Datenverarbeitungsvorgängen: *Wölfle*, Kontextsensitive Arbeitsassistenzsysteme zur Informationsbereitstellung in der Intralogistik, Dissertation, München, Technische Universität München, 2014, S. 50f, abrufbar unter http://www.fml.mw.tum.de/fml/images/Publikationen/Wölfle.pdf (zuletzt aufgerufen am 20.09.2017).

[198] Vgl. *Roßnagel*, MMR 2005, 71 (72), Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung.

zur Verfügung gestellt.[199] Auch in anderen Bereichen kann eine manuelle Eingabe erforderlich sein, so etwa bei der Auswahl bestimmter Menüpunkte.[200]

Es lässt sich mithin nicht pauschal konstatieren, dass beim Einsatz adaptiver Arbeitsassistenzsysteme stets eine Direkt- oder eine Dritterhebung erfolgt. Vielmehr muss anhand konkreter Anwendungsschritte die jeweils einschlägige Transparenzbestimmung ermittelt werden. Dies gilt insbesondere mit Blick auf die unterschiedlichen Fristen zur Informationsbereitstellung.

3.3.2.4 Informationspflichten bei Direkterhebung, Art. 13 DSGVO

3.3.2.4.1 Umfang

Die Informationspflichten bei der Direkterhebung ergeben sich aus Art. 13 DSGVO. Gemäß. Abs. 1 sind folgende Informationen erforderlich:

- der Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls dessen Vertreter (lit. a);
- die Kontaktdaten des Datenschutzbeauftragten, sofern es einen solchen gibt (lit. b); dabei dürfte die namentliche Nennung des Datenschutzbeauftragten nicht zwingend sein. Vielmehr dürfte auch eine generische Beschreibung der Organisationseinheit (datenschutzbeauftragte@) ausreichen;
- die Zwecke der Datenverarbeitung und die Rechtsgrundlage, auf der diese beruht (lit. c);
- das berechtigte Interesse des Verantwortlichen (lit d), sofern die Datenverarbeitung auf einer Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO beruht;
- bei einer geplanten Weitergabe der Daten, die Empfänger oder die Kategorien von Empfängern (lit. e);
- und schließlich bei einer Datenübermittlung in ein Drittland (etwa bei der Nutzung von US-Cloud-Diensten) oder an eine Internationale Organisation, die beabsichtigte Übermittlung wie auch das Vorliegen eines Angemessenheitsbeschlusses der Kommission (Art. 45 DSGVO) .[201]

In Art. 13 Abs. 2 DSGVO werden darüberhinausgehende Informationspflichten für die Direkterhebung normiert. Sie sind nur zu erteilen, wenn dies erforderlich ist, um eine faire und transparente Verarbeitung zu gewährleisten und umfassen folgende Informationen:

---

[199] *Wölfle*, Kontextsensitive Arbeitsassistenzsysteme zur Informationsbereitstellung in der Intralogistik, Dissertation, München, Technische Universität München, 2014, S. 53.

[200] *Wölfle*, Kontextsensitive Arbeitsassistenzsysteme zur Informationsbereitstellung in der Intralogistik, Dissertation, München, Technische Universität München, 2014, S. 55.

[201] Fehlt es an einem Angemessenheitsbeschluss, erstreckt sich die Informationspflicht auf die getroffenen Maßnahmen (Garantien nach Art. 46 DSGVO, verbindliche interne Datenschutzvorschriften nach Art. 47 DSGVO oder Beurteilungen nach Art. 49 Abs. 1 UAbs. 2 DSGVO). Ggf. müssen diese der betroffenen Person auch als Kopie zur Verfügung gestellt werden (Art. 13 Abs. 1 lit. f).

- die konkrete Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (lit. a);
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die sie betreffenden personenbezogenen Daten sowie auf Berichtigung, Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit (lit. b);
- wenn die Verarbeitung auf einer (zulässigen) Einwilligung (Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO) beruht: das Bestehen des Rechts, die Einwilligung jederzeit und mit Wirkung ‚ex nunc' zu widerrufen (lit. c);
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (lit. d);
- eine gesetzliche oder vertragliche Pflicht bzw. Erforderlichkeit zur Bereitstellung personenbezogener Daten sowie über die Konsequenzen der Nichtbereitstellung (lit. e) und
- das Bestehen automatisierter Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1 und 4 DSGVO und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (lit. f).[202]

Bei einer späteren Zweckänderung findet Art. 13 Abs. 3 DSGVO Anwendung, wonach diese zwar grundsätzlich möglich, der Betroffene aber über den neuen Zweck zu informieren ist. Zusätzlich wird erneut eine umfängliche Informationspflicht nach Abs. 2 ausgelöst.

3.3.2.4.2 Ausnahmen

3.3.2.4.2.1 Ausnahmen nach Art 13 Abs. 4 DSGVO

Sämtliche in den Art. 13 Abs. 1 und 2 DSGVO aufgeführten Informationspflichten entfallen, wenn der Betroffene bereits Kenntnis von den Informationen hat. Dabei genügt es nicht, dass die Verarbeitung branchenüblich ist.[203] Die Beweislast für die Kenntnis liegt beim Verantwortlichen.

3.3.2.4.2.2 Ausnahmen nach § 32 BDSG-neu

Auch hier ermöglicht die DSGVO dem nationalen Gesetzgeber unter bestimmten Voraussetzungen weitere Ausnahmetatbestände zu schaffen, vgl. Art. 23 DSGVO. Hiervon hat der deutsche Gesetzgeber in § 32 BDSG-neu Gebrauch gemacht. Die Ausnahmen spielen aber im Zusammenhang mit der Datenverarbeitung bei adaptiven Assistenzsystemen eher keine Rolle.

---

[202] Nicht in Bezug genommen ist damit das sogenannte „einfache Profiling" in Art. 4 Nr. 4 DSGVO, das eine Verarbeitung personenbezogener Daten darstellt, sondern nur die in Art. 22 DSGVO geregelte, auf einer automatisierten Verarbeitung beruhenden Entscheidung, die rechtliche Wirkung gegenüber der betroffenen Person entfaltet, oder sie in sonstiger Weise beeinträchtigt. Die Formulierung ‚involvierte Logik' dürfte sich insoweit mit dem des § 6a Abs. 3 BDSG-alt decken. Neu ist indes, dass dies nunmehr nicht mehr nur auf entsprechenden Antrag hin mitzuteilen, sondern als Informationspflicht ausgestaltet ist, die sich auch auf das Bestehen automatisierter Entscheidungsfindung und insbesondere auf ihre Tragweite und Auswirkungen bezieht.

[203] *Gola*/*Pötters*/*Wronka*, Handbuch Arbeitnehmerdatenschutz, 7. Auflage 2016, S. 414.

3.3.2.5 Informationspflichten bei „Dritterhebung“ / Erhebung aus anderen Quellen, Art. 14 DSGVO

3.3.2.5.1 Umfang

Die Datenerhebung aus anderen Quellen bzw. Dritterhebung ist mit erweiterten Informationspflichten verbunden. Zusätzlich zu den in Art. 13 Abs. 1 und 2 DSGVO aufgeführten Angaben fordert Art. 14 DSGVO weitergehende Informationen über:

- die Kategorien personenbezogener Daten, die verarbeitet werden (Abs. 1 lit. d);
- die Quelle, aus der die personenbezogenen Daten stammen und ggf. ob diese öffentlich zugänglich sind (Abs. 2 lit. f).[204]

3.3.2.5.2 Ausnahmen[205]

Bei der Dritterhebung beschränken sich die Ausnahmen nach Art. 14 Abs. 5 DSGVO auf

- die Kenntnis des Betroffenen (lit. a);
- die Unmöglichkeit oder Unverhältnismäßigkeit der Informationserteilung (lit b);
- das Vorliegen einer ausdrücklichen gesetzlichen Regelung, aus der sich das Recht des Verantwortlichen zur Erlangung oder Offenlegung der Daten des Betroffenen ergibt, sofern diese Norm geeignete Maßnahmen zum Schutz der berechtigten Interessen des Betroffenen enthält (lit. c);
- Vertraulichkeit der Informationen aufgrund eines unionsrechtlichen oder mitgliedsstaatlichen Berufsgeheimnisses einschließlich einer satzungsmäßigen Geheimhaltungspflicht (lit. d).

3.3.2.6 Informationspflicht bei mehreren Verantwortlichen, Art. 26 Abs. 1 DSGVO

Bei der Datenverarbeitung durch mehrere Verantwortliche[206] müssen sich diese, wie bereits oben angesprochen, in einer Vereinbarung darauf verständigen, wer für die Wahrung der Betroffenenrechte, insb. auch der Rechte aus Art. 13 und 14 DSGVO, verantwortlich ist (Art. 26 Abs. 1 DSGVO). Zur Wahrung des Transparenzgrundsatzes muss die dahingehende Vereinbarung der betroffenen Person zur Verfügung gestellt werden (Art. 26 Abs. 2 Satz 2 DSGVO). Die Aufgabe der Informationserteilung wie auch der Zuständigkeit für die Wahrung der Betroffenenrechte kann der Arbeitgeber nach der hier vertretenen Auffassung jedoch wegen seiner Fürsorgepflichten gegenüber dem Beschäftigten nicht auf den Hersteller übertragen.

3.3.2.7 Informationspflicht bei der Übermittlung an Auftragsverarbeiter

Nach dem BDSG-alt stellte die Weitergabe an Auftragsdatenverarbeiter regelmäßig keine Übermittlung dar, weil Auftragsdatenverarbeiter, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Ab-

---

[204] Ist dies nicht möglich, da verschiedene Quellen herangezogen wurden, so ergibt sich aus EG 61 DSGVO, dass diese Information auch allgemein gehalten werden kann und sollte.

[205] Weitere Ausnahmen ergeben sich aus § 29 und § 33 BDSG-neu, die aber für die hier zu begutachtende Frage keine Rolle spielen.

[206] vgl. E.II.2.

kommens über den europäischen Wirtschaftsraum (EWR) personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, nicht als „Dritte“ eingeordnet wurden (§ 3 Abs. 8 S. 2 und 3 BDSG a.F.). Deshalb war der Betroffene auch bei Unkenntnis von der „Übermittlung“ nicht zu benachrichtigen. Eine § 3 Abs. 8 S. 2 und 3 BDSG a.F. entsprechende Vorschrift existiert unter Geltung der DSGVO nicht. Mit Blick auf das Transparenzgebot stellt sich die Frage, ob der Beschäftigte darüber zu informieren ist, dass ein Auftragsverarbeiter eingeschaltet wird. Nach dem Wortlaut des Art. 14 Abs. 3 lit. c DSGVO löst die „Offenlegung an andere Empfänger“ die Informationspflicht aus. Aus Art. 4 Nr. 9 DSGVO ergibt sich, dass Empfänger sowohl ein Dritter als auch ein Auftragsverarbeiter sein kann. Deshalb ist bei jeder Übermittlung der Daten an einen Auftragsverarbeiter der Beschäftigte hierüber spätestens zum Zeitpunkt der ersten Offenlegung von seinem Arbeitgeber zu informieren.

3.3.3 Auskunftsanspruch / Recht auf Erhalt einer Kopie, Art. 15 DSGVO

Das bereits unter dem BDSG-alt bestehende Auskunftsrecht wird durch die DSGVO inhaltlich stark ausgeweitet und um ein Zugriffsrecht in der Form des Erhalts einer Kopie der personenbezogenen Daten ergänzt.

3.3.3.1 Das Recht auf Auskunft, Art. 15 Abs. 1 und 2 DSGVO

3.3.3.1.1 Umfang des Auskunftsrechts

Art. 15 DSGVO verleiht auch dem Beschäftigten ein zweistufiges Auskunftsrecht. Er kann von dem Verantwortlichen in einem ersten Schritt eine Bestätigung darüber verlangen, ob ihn betreffende personenbezogene Daten verarbeitet werden und – sofern dies der Fall ist – in einem zweiten Schritt Auskünfte hierzu verlangen. Ebenso wie nach § 34 Abs. 1 BDSG-alt erstreckt sich der Auskunftsanspruch inhaltlich auf:

- über die betroffene Person verarbeitete Daten (Art. 15 Abs. 1, 2. HS DSGVO);
- die Verarbeitungszwecke (Art. 15 Abs. 1 lit. a DSGVO),
- die Empfänger oder Kategorien von Empfängern (neu: insb. bei Empfängern in Drittländern oder bei internationalen Organisationen) (Art. 15 Abs. 1 lit. c DSGVO),
- im Falle der Dritterhebung: alle Informationen über die Herkunft der Daten (Art. 15 Abs. 1 lit. g DSGVO).

Darüber hinaus muss der Verantwortliche dem Betroffenen Informationen erteilen über:

- die Kategorien der personenbezogenen Daten (Art. 15 Abs. 1 lit. b DSGVO),
- die Speicherdauer, oder sofern diese nicht feststeht über die Kriterien der Festlegung selbiger (Art. 15 Abs. 1 lit. d) DSGVO),
- das Bestehen eines Rechts auf Berichtigung, Löschung, Einschränkung der Verarbeitung, oder eines Widerspruchsrechts (Art. 15 Abs. 1 lit. e DSGVO),
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde (Art. 15 Abs. 1 lit. f DSGVO),
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1, Abs. 4 DSGVO und aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person (Art. 15 Abs. 1 lit. h DSGVO),

- die Bezeichnung der geeigneten Garantien gem. Art. 46 DSGVO zur Wahrung eines angemessenen Datenschutzniveaus bei Übermittlungen in Drittländer oder an internationale Organisationen (Art. 15 Abs. 2 DSGVO).

Im Zusammenhang mit adaptiven Arbeitsassistenzsystemen kommt EG 63 Satz 6 DSGVO Bedeutung zu. Verantwortliche, die große Datenmengen verarbeiten, können verlangen, dass der Betroffene sein Auskunftsverlangen präzisiert. Das hat eine „inhaltliche“ und eine „prozessuale“ Folge. Zum einen führt dieses Recht, eine Präzisierung verlangen zu können, dazu, dass der Betroffene eine für ihn sinnvolle Auskunft erhält (und nicht etwa nicht zuordnen- und unüberschaubare Daten, mit denen er nichts anfangen kann). Zum anderen kann sich der Verantwortliche gegenüber dem Betroffenen auf dieses Recht berufen und muss, wenn der Betroffene sein Auskunftsverlangen nicht präzisiert, gar keine Auskunft erteilen.

3.3.3.1.2 Recht auf Erhalt einer Kopie, Art. 15 Abs. 3 und 4 DSGVO

Das Recht auf Auskunft wird in Art. 15 Abs. 3 DSGVO um das Recht auf Erhalt einer Kopie der personenbezogenen Daten ergänzt.

Anders als beim Recht auf Datenportabilität ist ein maschinenlesbares Format nicht geschuldet. Ausweislich EG 63 Satz 4 DSGVO kann der Verantwortliche seine Verpflichtung aus dem Zugriffsrecht auch erfüllen, indem der betroffenen Person per Fernzugang Zugriff auf ihre personenbezogenen Daten gewährt wird (z.B. im Rahmen eines persönlichen Nutzer-Accounts).

Gem. Art. 15 Abs. 4 DSGVO findet das Zugriffsrecht seine Schranken in den Rechten und Freiheiten Dritter. Als Beispiele hierfür nennt EG 63 Satz 5 Geschäftsgeheimnisse, die Rechte des geistigen Eigentums sowie das Urheberrecht an Software. Im Zusammenhang mit adaptiven Arbeitsassistenzsystemen kommen insbesondere auch Persönlichkeitsrechte anderer Beschäftigter in Betracht. Auch die Rechte Dritter sollen allerdings nicht dazu führen können, dass der betroffenen Person jegliche Auskunft verweigert wird (EG 63 Satz 6). Um die Rechte anderer Beschäftigter zu schützen, sind deren Daten mithin zu anonymisieren.

3.3.3.2 Ausnahmen

Die Ausnahme des Art. 15 Abs. 4 DSGVO betrifft nur die Kopie, nicht aber das Recht auf Auskunft allgemein. Das hätte zur Folge, dass eine Auskunft beispielsweise nicht unter Berufung auf Betriebs- und Geschäftsgeheimnisse verweigert werden dürfte. Dies hat gerade beim Einsatz adaptiver Assistenzsysteme erhebliche Auswirkungen. Die mittels der Assistenzsysteme verarbeiteten Beschäftigtendaten geben regelmäßig Aufschluss über die Betriebsorganisation. Die mit Hilfe einer Datenbrille erhobenen Daten zur Anweisung von Kommissionierungsaufgaben beispielsweise beinhalten nicht nur Informationen über den Beschäftigten, sondern gleichzeitig auch über die Arbeitsschritte, die Aufgaben, die Waren und Produkte, die Zeitpunkte und Reihenfolge des Anfahrens der Waren, die Häufigkeit, mit welcher bestimmte Produkte nachgefragt werden und vieles mehr. Derartige Informationen gehören zum Betriebsgeheimnis des Unternehmens.

In der Literatur wird daher überwiegend vertreten, dass es sich um eine planwidrige Regelungslücke handele und daher die Ausnahme aus Art. 15 Abs. 4 DSGVO auch

auf den Auskunftsanspruch insgesamt anwendbar sei.[207] Allerdings darf der Arbeitgeber die Auskunft in diesem Fall nicht insgesamt verweigern, sondern muss die Auskünfte erteilen, die nicht zu seinem Betriebsgeheimnis gehören.

Im Fall der Kommissionierung anhand von Datenbrillen wäre es also denkbar, dass der Arbeitgeber die Auskunft erteilt, dass er über den Beschäftigten Daten gespeichert hat, wonach er an einem bestimmten Tag bestimmte Arbeitsschritte zur Kommissionierung ausgeführt hat. Weitere Informationen müsste er dann nicht preisgeben.

In § 34 Abs. 1 Nr. 2 BDSG-neu findet sich zudem eine Unverhältnismäßigkeitsausnahme der Rechte auf Auskunft und Erhalt einer Kopie. Diese gilt für den Fall, dass die Beschäftigtendaten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, sie ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Bei adaptiven Arbeitsassistenzsystemen liegen diese Voraussetzungen in Ermangelung einer Aufbewahrungspflicht jedoch regelmäßig nicht vor.

Ein weiterer und im Zusammenhang mit adaptiven Arbeitsassistenzsystemen ggf. einschlägiger Fall der Unverhältnismäßigkeit findet sich in Art. 12 Abs. 6 i. V. m. Art. 11 Abs. 2 DSGVO. Danach finden die Betroffenenrechte keine Anwendung, wenn der Verantwortliche glaubhaft machen kann, dass die betroffene Person trotz zusätzlicher Bereitstellung identifizierender Informationen nicht zuordenbar ist. Teilweise wird – hergeleitet aus dem allgemeinen Grundsatz von Treu und Glauben – daneben eine generelle Ausnahme für Fälle unverhältnismäßigen Aufwands diskutiert.[208] Hier wäre aber eine restriktive Herangehensweise geboten. Schließlich ist der Verantwortliche nach Art. 25 DSGVO gehalten, seine Prozesse so zu gestalten, dass die Betroffenenrechte effektiv verwirklicht werden können. In jedem Fall wären die Gründe für die Auskunftsverweigerung zu dokumentieren und die Verweigerung zu begründen.[209]

3.4 Betroffenenrechte

3.4.1 Recht auf Berichtigung, Art. 16 DSGVO

Art. 16 DSGVO gibt dem Beschäftigten eine Korrekturmöglichkeit im Falle der Verarbeitung unrichtiger oder unvollständiger personenbezogener Daten an die Hand.

---

[207] *Schmidt-Wudy* in: Wolff/Brink BeckOK Datenschutzrecht, 22. Edition, Stand: 01.11.2017, Art 15, Rn. 97 (analoge Anwendung); *Paal* in: Paal/Pauly, DS-GVO, 2. Auflage 2018, Art. 15 Rn. 41 (unmittelbare Anwendung).

[208] *Franck* in: Gola, DS-GVO, 1. Auflage 2017, Art. 15, Rn. 30.

[209] Vgl. § 34 Abs. 2 BDSG-neu, Art. 12 Abs. 4 DSGVO.

3.4.2 Recht auf Löschung und Löschpflicht, Art. 17 Abs. 1 DSGVO

Von größerer Relevanz im Zusammenhang mit adaptiven Arbeitsassistenzsystemen dürften die in Art. 17 DSGVO verankerten Löschansprüche und -pflichten sein.

3.4.2.1 Recht des Betroffenen auf und Pflicht des Verantwortlichen zur Löschung

Art. 17 regelt zunächst in Abs. 1 das Recht des Betroffenen auf Löschung und die bereits aus dem deutschen Datenschutzrecht bekannte, damit korrespondierende Pflicht des Verantwortlichen, personenbezogene Daten unter bestimmten Voraussetzungen zu löschen. Löschanspruch und -pflicht bestehen, wenn

- die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art. 17 Abs. 1 lit. a DSGVO),
- die betroffene Person ihre Einwilligung, auf die sich die Verarbeitung gem. Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO stützt, widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt (Art. 17 Abs. 1 lit. b DSGVO),
- die betroffene Person gem. Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung einlegt und keine vorrangig berechtigten Gründe für die Verarbeitung vorliegen, oder die betroffene Person gem. Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung einlegt (Art. 17 Abs. 1 lit. c DSGVO),
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 lit. d DSGVO),
- die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, erforderlich ist (Art. 17 Abs. 1 lit. e DSGVO) oder
- die personenbezogenen Daten in Bezug auf angebotene Dienste der Informationsgesellschaft gem. Art. 8 Abs. 1 erhoben wurden (Art. 17 Abs. 1 lit. f DSGVO).

Von besonderer Bedeutung sind hier der Zweckfortfall bzw. Zweckerreichung. Wurden die personenbezogenen Daten beispielsweise ausschließlich erhoben, um die Kooperation mit einem virtuellen Team für ein abschließendes Projekt zu ermöglichen, sind die Daten nach Abschluss des Projekts zu löschen. Etwas anderes kann sich nach erfolgreicher Kompatibilitätsprüfung jedoch ergeben, wenn die Daten auch in anderen Projekten eingesetzt werden sollen. Um die Pflichten erfüllen zu können, sollte bereits bei der Entwicklung und erstem Einsatz adaptiver Arbeitsassistenzsysteme wirksame Löschkonzepte entwickelt werden.

3.4.2.2 Ausnahmen

Eine im Zusammenhang mit adaptiven Arbeitsassistenzsystemen relevante Ausnahme von der Löschpflicht könnte § 35 Abs. 1 BDSG-neu sein. Dieser greift in Fällen, in denen die Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Auch hier ist jedoch mit Blick auf Art. 25 DSGVO eine restriktive Betrachtung geboten. Jedenfalls tritt aber an die Stelle des Löschanspruchs dann das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO. Der Verantwortliche muss die betroffene Person nach Art. 12 Abs. 4 DSGVO entsprechend unterrichten.

3.4.3 Recht auf Datenportabilität, Art. 20 DSGVO

Mit der DSGVO wird erstmals ein Anspruch des Betroffenen auf Datenportabilität eingeführt. Art. 20 DSGVO sieht vor, dass der Betroffene alle ihn betreffenden personenbezogene Daten, die er an den Verantwortlichen übermittelt hat, in einem strukturierten, gängigen und maschinenlesbaren Format (z.B. als CD oder USB-Stick) herausverlangen (Abs. 1) oder einem anderen Verantwortlichen übermitteln lassen kann (Abs. 2).

Das Recht auf Datenportabilität soll es für den Betroffenen vereinfachen, ohne Behinderung des bisherigen Verantwortlichen mit seinen personenbezogenen Daten zu einem neuen Anbieter zu wechseln[210]. Der Gesetzgeber hatte bei der Einführung des Rechts insbesondere die Portabilität der Daten aus sozialen Netzwerken und die Erleichterung des Anbieterwechsels im Blick. Gleichwohl wurde der Anwendungsbereich der Vorschrift auf jeden Verantwortlichen ausgedehnt, weshalb sie auch im Beschäftigtenkontext Relevanz entfaltet.

Für das Recht auf Datenübertragbarkeit müssen vier wesentliche Voraussetzungen kumulativ erfüllt sein:

- Es muss sich um personenbezogene Daten handeln,
- die von dem Betroffenen dem Verantwortlichen bereitgestellt worden sind,
- die Verarbeitung muss auf einer Einwilligung oder in Anwendung von § 26 BDSG-neu erfolgen und damit der Erfüllung des Arbeitsvertrages dienen, sowie
- mithilfe automatisierter Verfahren erfolgen.

Von zentraler Bedeutung für die Reichweite der Verpflichtung ist die zweite Voraussetzung das „Bereitstellen“ durch den Betroffenen. Insoweit ist insbesondere umstritten, ob es insoweit einer aktiven Handlung der betroffenen Person bedarf, oder es ausreicht, wenn Daten durch bloßes Beobachten der betroffenen Person (etwa in Form von Tracking) durch den Verantwortlichen anfallen (sog. observed data). Die Artikel 29 Datenschutzgruppe geht von einem weiten Begriffsverständnis aus und hält das Recht auf Datenportabilität auch bei „observed data“ uneingeschränkt für anwendbar.[211] Indes spricht der Wortlaut der Norm für eine einschränkende Interpretation, wonach „Bereitstellen“ ein aktives Verhalten der betroffenen Person voraussetzt.[212] Auch die Systematik der Betroffenenrechte legt eine restriktive Auslegung nahe. Weder das Auskunftsrecht (Art. 15 DSGVO) noch der Löschungsanspruch (Art. 17 DSGVO) sind auf Daten beschränkt, die der Betroffene bereitgestellt hat. Die Regelungen sind ihrem Wortlaut nach vielmehr auf sämtliche beim Verantwortlichen vorhandene personenbezogene Daten der betroffenen Person anwendbar. Es dürfte daher dem erkennbaren Willen des Gesetzgebers entsprechen, den Umfang der vom

---

[210] *Däubler* in: Gläserne Belegschaften, 7. Auflage 2017, Rn. 545a m.w.N.

[211] Artikel 29 Datenschutzgruppe, Guidelines on the right to data portability WP 16/EN/242, S. 8f; dies kritisch sehen: *Piltz* in: Gola, DS-GVO, 1. Auflage 2017, Art. 20, Rn. 14.

[212] So unter Berücksichtigung der deutschen, englischen, französischen und spanischen Sprachfassung zutreffend *Strubel*, ZD 2017, 355 (357 f.); vgl. ferner *Brüggemann*, DSRITB 2017, 1 (4).

Recht auf Datenportabilität erfassten Daten gegenüber den übrigen Betroffenenrechten zu beschränken.[213]

Hingegen sprechen Sinn und Zweck von Art. 20 DSGO dafür, auch „observed data" grundsätzlich über Art. 20 DSGO zu erfassen. Aus Erwägungsgrund 68 folgt, dass der primäre Regelungszweck von Art. 20 DSGVO darin besteht, der betroffenen Person „bessere Kontrolle über die eigenen Daten" zu verschaffen und es ihm zu ermöglichen diese Daten an „einen anderen Verantwortlichen zu übermitteln". Die hierdurch geschaffene Dispositionsfähigkeit ermöglicht es der betroffenen Person, selbständig darüber zu entscheiden, durch wen eine Auswertung ihrer Daten erfolgt. Als Regelungsreflex sollen auf diese Weise zudem sog. „lock-in" Effekte vermieden werden.[214] Hierdurch soll dem Betroffenen etwa der Wechsel zwischen verschiedenen sozialen Netzwerken erleichtert werden.[215] Das Bedürfnis nach mehr Kontrolle über die Daten – etwa im Zusammenhang mit einem Anbieterwechsel – kann aber auch und gerade dann bestehen, wenn es um Daten geht, die aus der Beobachtung des Verhaltens des Betroffenen gewonnen werden.[216] Denn auch solche Daten können für die Inanspruchnahme einer Leistung durch den Betroffenen und für einen entsprechenden Anbieterwechsel von Bedeutung sein. Die bloße Unterscheidung danach, ob die Daten von der betroffenen Person aktiv zur Verfügung gestellt werden oder aus einer Beobachtung des Betroffenen stammen, erscheint daher als Kriterium für eine einschränkende Auslegung ungeeignet.

Ausgehend vom Regelungszweck der Norm dürfte bei der Anwendung des Rechts auf Datenportabilität vielmehr danach zu differenzieren sein, ob die Daten desjenigen, der das Recht geltend macht, auch im Verhältnis zu andern Verantwortlichen für vergleichbare Leistungen typischerweise genutzt werden können.[217] Dies kann sowohl aktiv zur Verfügung gestellte Daten der betroffenen Person betreffen als auch solche, die durch Beobachtung gewonnen werden.

Legt man dieses Verständnis zugrunde, könnte der Anbieter einer Fitness-App etwa verpflichtet sein, einem Nutzer auf dessen Wunsch hin sowohl die Registrierungsdaten (Name, Adresse, Bankverbindung etc.) als auch „observed data" wie z.B. zu absolvierten Laufstrecken in einem gängigen Format zur Verfügung zu stellen. Daten die mit den ausgetauschten Leistungen allenfalls mittelbar in Zusammenhang stehen – etwa Informationen, die der Anbieter zu Werbezwecken erhebt – fallen danach aber nicht in den Anwendungsbereich der Regelung.[218] Gleiches muss für Daten gelten, von denen typischerweise nicht erwartet werden kann, dass diese auch im Verhältnis zu einem anderen Anbieter sinnvoll verarbeitet werden können.

Übertragen auf den Beschäftigtenkontext bedeutet dies, dass bestimmte Daten aus Personaldatensystemen (z.B. Stammdaten, Informationen zur Ausbildung, Angaben zur Sozialversicherung) dem Anspruch auf Datenportabilität unterfallen können –

---

[213] *Brüggemann*, DSRITB 2017, 1 (4).
[214] *Strubel*, ZD 2017, 355 (357); *Paal* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 20, Rn. 6.
[215] *Härting* BB 2012, 459 (465); *Paal* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 20, Rn. 6 m.w.N.
[216] So mit Blick auf die Nutzung von Fitnessarmbändern zutreffend *Brüggemann*, DSRITB 2017, 1 (5).
[217] In diese Richtung auch *Brüggemann*, DSRITB 2017, 1; *Strubel*, ZD 2017, 355.
[218] *Brüggemann*, DSRITB 2017, 1 (6).

etwa um einen Arbeitgeberwechsel zu erleichtern.[219] Hingegen dürften Daten, die im Rahmen der Anwendung adaptiver Assistenzsysteme gewonnen werden, in aller Regel nicht vom Anwendungsbereich des Art. 20 DSGVO erfasst sein. Der Einsatz solcher Systeme steht gerade erst am Anfang. Typischerweise sind die dabei erhobenen Informationen stark von der konkret eingesetzten Technologie abhängig und dürften schon aus diesem Grund für andere Arbeitgeber kaum sinnvoll einsetzbar sein. Stellt man – wie hier vorgeschlagen – auf eine typisierende Betrachtung des jeweiligen Verhältnisses zwischen dem Verantwortlichen und dem Betroffenen ab, fehlt es daher in aller Regel bereits an einer sinnvollen Verwendungsmöglichkeit für solche Daten. Ein berechtigtes Interesse der betroffenen Person an der Übertragbarkeit auf einen anderen Arbeitgeber wird man in einer solchen Konstellation daher nicht annehmen können.

In Ausnahmefällen könnte allerdings ein berechtigtes Interesse des Beschäftigten an der Mitnahme von ihn betreffenden Daten aus seiner Tätigkeit mit adaptiven Assistenzsystemen bestehen. Zu denken wären beispielsweise an selbstlernende Systeme, die auf Körpergröße, Interaktionen, Sprache und anderen personalisierten Merkmalen basieren. Der Beschäftigte könnte diese Erkenntnisse ggf. auch für seinen neuen Arbeitsplatz nutzen. Gegen einen Anspruch auf Mitnahme dieser Daten spricht jedoch das Interesse des Arbeitgebers, dass betriebsinterne Informationen nicht an einen Dritten, möglicherweise gar an einen Wettbewerber, weitergegeben werden. Art. 20 Abs. 4 DSGVO sieht daher, entsprechend der Ausnahme für einen Auskunftsanspruch, auch hier vor, dass das Recht auf Datenportabilität nicht besteht, wenn dadurch Rechte und Freiheiten Dritter beeinträchtigt werden. Erkenntnisse aus der Anwendung adaptiver Assistenzsysteme werden im Regelfall Betriebsgeheimnisse darstellen. Aber auch unterhalb der Schwelle eines Betriebsgeheimnisses überwiegen die Interessen des Arbeitgebers, dass Informationen zu internen Betriebsabläufen nicht an die Konkurrenz gehen. Der Beschäftigte wird sich daher im Regelfall nicht auf das Recht der Datenportabilität berufen können, um ihn betreffende Daten, die im Rahmen der Arbeitsausführung anfallen, zu seinem neuen Arbeitgeber mitzunehmen. [220]

3.5 Sonstige Hinweis- und Benachrichtigungspflichten

3.5.1 Hinweispflicht auf bestehendes Widerspruchsrecht, Art. 21 Abs. 4 DSGVO

Der Arbeitgeber muss den Beschäftigten im Falle eines Widerspruchsrechts in gesonderter, d.h. von sonstigen Informationen klar getrennter Form ausdrücklich und unmissverständlich auf das Bestehen des Widerspruchsrechts gem. Art. 21 Abs. 1 und 2 DSGVO hinweisen. Dies gilt insb. bei einer auf ein berechtigtes Interesse gestützten Verarbeitung sowie beim Profiling[221].

---

[219] In diese Richtung *Paal* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 20 Rn. 6; *Wybitul/Fladung*, BB 2012, 509 (512); kritisch *Däubler*, in: Gläserne Belegschaften, 7. Auflage 2017, Rn. 545b.

[220] Pilz, RDV 2018, 3 (7).

[221] vgl. D.II.4.

Hierbei gilt die Frist des Art. 12 Abs. 3 DSGVO, wonach die Information grundsätzlich unverzüglich, spätestens jedoch innerhalb eines Monats zu erteilen ist.

3.5.2 Benachrichtigungspflichten im Falle eines „Datenlecks“, Art. 33, 34 DSGVO

Auch nach der DSGVO sind umfangreiche Benachrichtigungspflichten im Falle eines Datenlecks sowohl gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) als auch gegenüber der betroffenen Person (Art. 34 DSGVO) zu erfüllen. Dies gilt in allen Fällen der Verletzung personenbezogener Daten, etwa durch Vernichtung, Verlust, Veränderung oder Offenlegung. Die Informationspflicht gilt stets gegenüber der Aufsichtsbehörde, gegenüber dem Betroffenen jedoch nur im Falle des Vorliegens eines erhöhten Risikos.

Neu ist insbesondere die Frist von 72 Stunden nach Bekanntwerden der Verletzung personenbezogener Daten gegenüber der Aufsichtsbehörde, die bei Nichteinhaltung besonders zu begründen ist (Art. 33 Abs. 1 DSGVO) sowie eine eigene Benachrichtigungspflicht des Auftragsverarbeiters (Art. 33 Abs. 2 DSGVO). Zudem treffen den Verantwortlichen umfangreiche Dokumentationspflichten (Art. 33 Abs. 5 DSGVO) zur Überprüfung durch die Aufsichtsbehörden. Die abschließende Entscheidung über das Vorliegen einer Ausnahme nach Art. 34 Abs. 3 lit. a-c DSGVO von der Benachrichtigungspflicht gegenüber dem Betroffenen bleibt der Aufsichtsbehörde vorbehalten (Art. 34 Abs. 4 DSGVO).

3.6 Sanktionen

Ein Verstoß gegen die Rechte der betroffenen Person in Art. 12-22 DSGVO kann gem. Art. 83 Abs. 5 lit. b DSGVO mit Geldbußen von bis zu EUR 20.000.000,00 oder im Fall eines Unternehmens von bis zu 4 % seines gesamten Jahresumsatzes geahndet werden. Daneben drohen – neben Reputationsschäden – Abmahnungen und Klagen durch Mitbewerber, Verbraucherzentralen und Verbände.

4 Technischer Datenschutz

Art. 25 Abs. 1 DSGVO verpflichtet den Verantwortlichen, technische und organisatorische Maßnahmen zu treffen, um die Grundsätze der DSGVO wirksam umzusetzen und die Rechte der betroffenen Personen zu schützen („Privacy by Design"). Daneben hat der Verantwortliche nach Art. 25 Abs. 2 DSGVO durch datenschutzfreundliche Voreinstellungen sicherzustellen, dass nur die für den jeweiligen Verarbeitungszweck erforderlichen Daten verarbeitet werden („Privacy by Default").[222]

4.1 Hintergrund

Die Konzepte des technischen Datenschutzes werden in der Literatur ebenso wie in der Praxis schon seit geraumer Zeit diskutiert.[223] Die Diskussion basiert auf folgenden Überlegungen:

Zum einen soll der Datenschutz bereits vor der tatsächlichen Datenverarbeitung beginnen. Schon bei der Konzipierung und Programmierung datenverarbeitender Systeme können wichtige und z.T. unumkehrbare Weichen für eine spätere möglichst datensensible Handhabe gestellt werden. Auch die organisatorischen Maßnahmen zur prozeduralen Sicherung der in Art. 5 Abs. 1 DSGVO verankerten datenschutzrechtlichen Grundsätze sollen bereits im Vorfeld getroffen werden.[224]

Zum anderen soll durch datenschutzfreundliche Technikgestaltung und Voreinstellungen auch ohne Mitwirkung der Betroffenen der Schutz ihrer Rechte gefördert werden. Ein derartig weitreichender Betroffenenschutz ist angezeigt, weil dem Einzelnen aufgrund der Komplexität moderner Datenverarbeitungsvorgänge oft nichts anderes übrigbleibt, als auf die Einhaltung der rechtlichen Vorgaben zu vertrauen. Dem liegt die Beobachtung zugrunde, dass der Einzelne, auch wenn er den Schutz seiner Privatsphäre abstrakt als wichtig einschätzt, sich in der Praxis häufig nicht entsprechend datensensibel verhält (sog. „Privacy Paradox").[225] Gerade auch im Beschäftigtenkontext werden Beschäftigte häufig auf eine funktionierende Compliance-

---

[222] Im englischsprachigen Verordnungstext wird der Begriff „Data Protection by Design and by Default" verwendet. Damit dürfte der europäische Gesetzgeber das Ziel verfolgt haben, herauszustellen, dass es primär um den Schutz der personenbezogenen Daten und nicht der Privatsphäre der Betroffenen geht. Dennoch hat sich die Bezeichnung Privacy by Design and by Default auch im deutschen Sprachraum durchgesetzt, Vgl. *Baumgartner/Gausling* ZD 2017, 308 (309).

[223] So wurde Privacy by Design and by Default jedenfalls im angloamerikanischen Raum schon in den 1990er Jahren aufgegriffen, s. *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 1; *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25, Rn. 38; Vgl. außerdem *Martini* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 8; *Hornung* ZD 2011, 51.

[224] Organisatorische Maßnahmen betreffen dabei im Gegensatz zu technischen nicht den Datenverarbeitungsvorgang selbst, sondern dessen äußere Rahmenbedingungen, s. *Baumgartner/Gausling* ZD 2017, 308 (310); für Beispiele technischer und organisatorischer Maßnahmen in diesem Sinne, Vgl. *Martini* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 28.

[225] Vgl. *Martini* in: Paal/Pauly, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 12; Schantz/Wolff/Wolff, 1. Auflage, DSGVO, Rn. 471.

Organisation des Unternehmens vertrauen oder aber aufgrund des Abhängigkeitsverhältnisses ihr informationelles Selbstbestimmungsrecht nicht oder nur unzureichend wahrnehmen. Unternehmer haben zudem häufig ein Interesse daran, Daten zu sammeln. Gerade im Kontext der Industrie 4.0 basieren viele Überlegungen auf Big Data-Anwendung, bei der Daten aus allen Unternehmensbereichen gesammelt und entsprechend ausgewertet werden.

Ein Mittel, dieser Gefahr für den Datenschutz zu begegnen, soll der sanktionsbewehrte technische Datenschutz darstellen. Die Verantwortlichen werden veranlasst, sog. „Privacy Enhancing Technologies“ zu integrieren oder ihre Voreinstellungen nicht am Maßstab der ökonomischen Nutzenmaximierung, sondern dem Grundsatz der Datenminimierung entsprechend zu gestalten. Die schon vor dem Inkrafttreten der DSGVO nationalrechtlich kodifizierten Grundsätze der Datenvermeidung und Datensparsamkeit sollen damit praktisch umgesetzt werden.[226]

4.2 Neuerungen durch die DSGVO

Im BDSG-alt gab es noch keine der Art. 25 DSGVO entsprechende Regelung. Der Verantwortliche musste zwar auch nach § 9 BDSG-alt technische und organisatorische Maßnahmen zu Gunsten eines präventiven Datenschutzes treffen. Diese Vorschrift setzte aber noch nicht an der Technikgestaltung oder datenschutzfreundlichen Voreinstellungen an.[227] In § 3 a BDSG-alt waren zumindest die Grundsätze der Datenvermeidung und Datensparsamkeit festgeschrieben, die auch im Mittelpunkt des technischen Datenschutzes stehen.[228] Aufgrund der fehlenden Sanktionsmöglichkeiten stellten diese Grundsätze aber lediglich unverbindliche Programmsätze dar.[229] Der technische Datenschutz der DSGVO geht demnach über diese Regelungen in zweifacher Hinsicht hinaus: Zum einen werden konkretere Vorgaben für präventive Maßnahmen gestellt, die insbesondere zur Sicherstellung der Datenminimierung erforderlich sind. Zum anderen wird der Stellenwert des technischen Datenschutzes durch eine entsprechende Sanktionsbewehrung deutlich erhöht.

Gerade bei technischen Neuerungen durch adaptive Assistenzsysteme werden daher diese neuen Grundsätze des technischen Datenschutzes eine große Rolle spielen.

---

[226] *Gierschmann* ZD 2016, 51 (53) *Thode* CR 2016, 714 (719); *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25, Rn. 7.

[227] *Baumgartner* in: Ehmann/Selmayr, 1. Auflage 2017, DSGVO Art. 25, Rn. 7.

[228] Vgl. *Hartung* in: Kühling/Buchner, 1. Auflage 2017, DSGVO Art. 25, Rn. 3.; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25, Rn. 9.

[229] *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 3; *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 7; Sydow/Kring ZD 2014, 271 (275).

4.3 Systematik

Art. 24 Abs. 1 DSGVO legt den Pflichtenkreis der Verantwortlichen fest: Diese haben geeignete technische und organisatorische Maßnahmen zu treffen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Datenverarbeitung gemäß der Verordnung erfolgt. Dieser abstrakte Pflichtenkanon soll im Einzelfall risikobasiert festgelegt werden.[230] Die Vorschriften zum Privacy by Design and by Default i.S.v. Art. 25 DSGVO konkretisieren diese Generalnorm und stellen in ihrem Anwendungsbereich lex specialis dar.[231]

Art. 25 Abs. 1 enthält dabei die allgemeine Verpflichtung der Verantwortlichen, den Anforderungen der DSGVO durch Technikgestaltung nachzukommen. Art. 25 Abs. 2 betrifft den Fall, dass der Betroffene durch Einstellungen selbst Einfluss auf die Datenverarbeitung nehmen kann und statuiert eine datenschonende Voreinstellung.[232]

Diese Normen stehen in einer engen Wechselbeziehung zur Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Eine solche ist immer durchzuführen, wenn eine Form der Verarbeitung für die Betroffenen voraussichtlich ein hohes Risiko hat, insbesondere bei Verwendung neuer Technologien. In der Praxis wird die von Art. 25 DSGVO geforderte Risikoanalyse die Datenschutz-Folgenabschätzung aus Art. 35 DSGVO in vielen Fällen vorwegnehmen, da diese zeitlich vor der Datenverarbeitung ansetzt.[233]

Der ähnliche Wortlaut macht zudem eine Abgrenzung zu Art. 32 DSGVO notwendig. Diese Vorschrift konkretisiert die Anforderungen an die Datensicherheit. Durch die Etablierung eines angemessenen Schutzniveaus sollen die Betroffenen insbesondere vor sicherheitsrelevanter Vernichtung, Verlust und unbefugter Offenlegung bereits erhobener Daten geschützt werden. Bei der Umsetzung dieser beiden Zielvorgaben bestehen aber zahlreiche Überschneidungen. Dies wird schon dadurch deutlich, dass die Pseudonymisierung als für die jeweilige Zwecke geeignetes Mittel sowohl in Art. 25 Abs. 1 DSGVO also auch in Art. 32 Abs. 1 lit. a DSGVO explizit genannt wird. Im Unterschied zum technischen Datenschutz werden durch Art. 32 DSGVO nicht nur der Verantwortliche, sondern auch der Auftragsverarbeiter verpflichtet.[234]

Die deutsche Vorschrift zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in § 71 BSDG-neu entspricht dem Wortlaut von Art. 25 DSGVO bis auf wenige sprachliche Änderungen. Aufgrund des vollharmoni-

---

[230] Vgl. zu diesem risikobasierten Ansatz *Piltz* K&R 2016, 709 (710 f.); *Veil* ZD 2015, 347 ff.

[231] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 24 Rn. 1.

[232] *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 9; *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 13; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25, Rn. 7.

[233] *Baumgartner* in: Ehmann/Selmayr, 1. Auflage 2017, DSGVO Art. 25 Rn. 3; *Plath* in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 25 Rn. 2.

[234] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 32 Rn. 8; zu den unterschiedlichen Regelungszwecken, s. auch *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25, Rn. 7; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 32 Rn. 1; *Hartung* in: Kühling/Buchner, 1. Auflage 2017, DSGVO Art. 25 Rn. 15; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 6.

sierenden Charakters der DSGVO und mangels einschlägiger Öffnungsklausel orientieren wir uns nachfolgend an dem Wortlaut der DSGVO.

4.4 Normadressat

Normadressat von Art. 25 DSGVO ist allein der Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO und nicht etwa der Hersteller von datenverarbeitenden Produkten, Diensten oder Anwendungen.[235] Der verantwortliche Arbeitgeber hat zumeist aber nur einen mittelbaren Einfluss auf die Entwicklung entsprechender Systeme. Dieses Spannungsfeld greift der Erwägungsgrund 78 S. 4 DSGVO auf, wonach die Verantwortlichen die Hersteller ermutigen sollen, in Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung datenschutzfreundliche Lösungen zu finden. Dem soll schon bei öffentlichen Ausschreibungen Rechnung getragen werden.[236] Hintergrund dieser Regelung ist die Vorstellung, dass die entsprechenden Herstellerleistungen durch den Einfluss und die Nachfrage ihrer Abnehmer gesteuert werden. Durch die erheblichen Sanktionen, die Verantwortlichen bei einer Missachtung des technischen Datenschutzes nach Art. 83 Abs. 4 lit. a DSGVO drohen, soll eine entsprechende Einflussnahme zur Entwicklung datenschutzfreundlicher Produkte durch die später Verantwortlichen gewährleistet werden.[237]

4.5 Datenschutz durch Technikgestaltung

Nach Art. 25 Abs. 1 DSGVO sollen sowohl zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der eigentlichen Verarbeitung technische und organisatorische Maßnahmen zur Umsetzung der Datenschutzgrundsätze, wie etwa der Datenminimierung, getroffen werden. Diese Vorgaben müssen bereits im Rahmen der Entwicklung der datenverarbeitenden Systeme berücksichtigt werden, da die eingesetzte Hard- und Software die anschließende Verwendung zum Großteil vorgibt.[238] In diesem Zusammenhang sollen auch die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen der DSGVO gerecht zu werden und die Rechte der betroffenen Personen zu schützen.

---

[235] Dies wird teilweise scharf kritisiert, s. *Baumgartner/Gausling* ZD 2017, 308 (311); *Schnatz* NJW 2016, 1841 (1845); Sydow/Kring ZD 2014, 271 (274); *Roßnagel/Richter/Nebel* ZD 2013, 103 (105 f.); *Hornung* ZD 2011, 51 (52); *Wolff* in: Schantz/Wolff DS-GVO, 1. Aufl., , Rn. 836; Auer-Reinsdorff/Conrad/*Conrad* § 33 Rn. 220 und § 34 Rn. 62; *Scholz* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3a Rn. 18b.

[236] Nach dem Entwurf des Europäischen Parlaments sollte dieser Passus sogar im Verordnungstext aufgenommen werden, Vgl. *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 17; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 81.

[237] Vgl. *Rose* ZD 2017, 64 (68); *Baumgartner/Gausling* ZD 2017, 308 (311); Gierschmann ZD 2016, 51 (53); *Thode* CR 2016, 714 (720); *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 5; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 25 Rn. 25; *Plath* in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 25 Rn. 7; *Hartung* in: Kühling/Buchner DS-GVO, 1. Auflage 2017, Art. 25 Rn. 13; *Mantz* in: Sydow, 1. Auflage 2017, DS-GVO, Art. 25 Rn. 79; *Schneider*, 1. Auflage, Datenschutz nach der DSGVO, 186.

[238] *Baumgartner/Gausling* ZD 2017, 308 (309); Auer-Reinsdorff/Conrad/*Conrad/Hausen* § 36 Rn. 165.

4.5.1 Abwägung

Das im Einzelfall gebotene Pflichtenniveau ist Ergebnis einer kontext-, risiko- und kostenabhängigen Abwägung.[239]

4.5.1.1 Risiken für die Rechte und Freiheiten der Betroffenen

Art. 25 Abs. 1 DSGVO schreibt vor, dass bei der Frage der Technikgestaltung die mit einer Datenverarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen sind. Da jede Datenverarbeitung risikobehaftet ist, muss im Einzelfall jeweils die Schwere dieses Risikos abgeschätzt werden. Maßgeblich dafür sind insbesondere zwei Kriterien: Die Eintrittswahrscheinlichkeit und die im gegebenen Fall zu erwartende Schadenshöhe.[240] Demnach sind an die Maßnahmen zur Technikgestaltung umso höhere Anforderungen zu stellen, je schwerer die Risiken für die Rechte und Freiheiten der Betroffenen im Einzelfall wiegen.[241]

Entsprechend einer Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DSGVO steht am Anfang dieser Analyse die Definition von Schutzzielen und die Identifikation und Bewertung von Risiken. Aus dem Erwägungsgrund 76 DSGVO ergibt sich, dass der Verantwortliche die Datenverarbeitung zumindest innerhalb der Kategorien geringes, mittleres und hohes Risiko einordnen muss.[242] Die besondere Prüftiefe und die weiten Dokumentationspflichten aus Art. 35 DSGVO dürften auch im Bereich des technischen Datenschutzes nur angezeigt sein, wenn im Einzelfall „voraussichtlich ein hohes Risiko“ besteht.[243] Ein solches ergibt sich aus der Sicht des Betroffenen, wenn Art, Umfang und Häufigkeit der Datenverarbeitung eine Schädigung oder Beeinträchtigung seiner persönlichen Rechte und Freiheiten mit sich bringen können.[244]

Aus dieser Wechselbeziehung zwischen der jeweiligen Verarbeitungssituation und dem entsprechenden Risiko für den Betroffenen folgt, dass die Verarbeitung von besonderen Kategorien von Daten nach Art. 9 DSGVO i.d.R. einen hohen Standard an den technischen Datenschutz erforderlich macht. Daneben stellt z.B. die Automatisierung des Verarbeitungsvorgangs ein Indiz für dessen hohes Risiko dar.[245] Ein weiterer Anknüpfungspunkt ist, ob mit dem System persönliche Aspekte des Betroffenen bewertet werden können. Dafür werden in Erwägungsgrund 75 DSGVO u.a. die Arbeitsleistung, die Zuverlässigkeit oder das Verhalten im Allgemeinen genannt. Für den Einzelnen ist es zudem mit einem hohen Risiko verbunden, wenn sein Aufenthaltsort sowie Ortswechsel analysiert oder sogar prognostiziert werden können, etwa

---

[239] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 25 Rn. 36.
[240] Vgl. zur objektiven Risikobewertung *Paulus* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 1.2.2017, DSGVO Art. 25 Rn. 7; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 21 ff.
[241] *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25, Rn. 21; *Martini* in: Paal/Pauly, 1. Auflage 2017, DS-GVO BDSG Art. 25 Rn. 37.
[242] *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 23.
[243] *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 24.; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 21.
[244] Vgl. Erwägungsgrund 94 DSGVO.
[245] *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 41.

um damit persönliche Profile zu erstellen. Dies ist insbesondere bei „Wearables“ möglich.[246]

4.5.1.2 Begrenzende Faktoren

Eine Berücksichtigung der Interessen der Betroffenen soll nach Art. 25 Abs. 1 DSGVO im Rahmen der Abwägung ihre Grenzen im Stand der Technik und den Implementierungskosten finden können. Somit gilt keine datenschutzfreundliche Technikgestaltung um jeden Preis. Diese Begrenzung ist Ausfluss des Verhältnismäßigkeitsprinzips aus Art. 52 Abs. 1 S. 2 GRCh.[247]

4.5.1.2.1 Stand der Technik

Die Berücksichtigung des Stands der Technik bedeutet, dass der Arbeitgeber solche vorhandenen technischen Möglichkeiten zu nutzen muss, die auf gesicherten Erkenntnissen von Wissenschaft und Technik basieren und im ausreichenden Maße zur Verfügung stehen.[248] In der Regel wird es sich dabei also um Techniken handeln, die bereits eine gewisse Erprobung durchlaufen haben. Es handelt sich bei diesem Begriff insofern um einen aus der Perspektive des Verantwortlichen begrenzenden Faktor, als dass gerade nicht die beste verfügbare Technik gefordert wird.[249] Die starre Pflicht der Verantwortlichen, stets die effektivsten und am weitesten entwickelten Methoden des technischen Datenschutzes verwenden zu müssen, würde der in Art. 25 DSGVO geforderten risikobasierten Verhältnismäßigkeitsprüfung im Einzelfall entgegen stehen. Bei der Bestimmung des Stands der Technik dürfte es für den Verantwortlichen empfehlenswert sein, sich an den Bewertungen der ENISA[250] und des Europäischen Datenschutzausschusses zu orientieren.[251] Durch die Bezugnahme auf diesen dynamischen Rechtsbegriff wird nochmals verdeutlicht, dass die Verantwortlichen die Maßnahmen zur Technikgestaltung fortlaufend überprüfen und an neue Entwicklungen anpassen müssen.[252]

4.5.1.2.2 Implementierungskosten

Die Verwendung des Begriffs der Implementierungskosten legt nahe, dass der europäische Gesetzgeber etwaige Folgekosten nicht als einen das Anforderungsniveau limitierenden Faktor ansieht.[253] Mit einer auf die Umsetzungskosten gestützten Argumentation soll der Verantwortliche danach nur verhindern können, Maßnahmen treffen zu müssen, die angesichts der geringen datenschutzrechtlichen Vorteile unverhältnismäßig sind. Somit kann im Einzelfall auch eine Entscheidung gegen die am

---

[246] *Weichert,* NZA 2017, 565 (569).
[247] *Martini* in: Paal/Pauly, 1. Auflage 2017, DS-GVO BDSG Art. 25 Rn. 38.
[248] *Baumgartner/Gausling* ZD 2017, 308 (309); *Schaffland/Holthaus* in: Schaffland/Wiltfang DS-GVO, Stand: 01.05.2017, Art. 25 Rn. 8; *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 22; *Ernestus* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014 § 9 Rn. 171.
[249] *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 38.
[250] Dieses Akronym steht für die European Union Agency for Network and Information Security.
[251] *Mantz* in: Sydow , 1. Auflage 2017, DSGVO, Art. 25 Rn. 39.
[252] *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 11; *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017 Art. 25 Rn. 22.
[253] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 25 Rn. 41; *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 11; Kühling/Buchner/*Hartung*, 1. Aufl., DSGVO Art. 25 Rn. 22; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 45.

Maßstab des Datenschutzes gemessen optimale Maßnahme im Einklang mit Art. 25 Abs. 1 DSGVO stehen. Dem Verantwortlichen soll durch einen Verweis auf möglicherweise anfallende langfristige Kosten aber keine Handhabe geben werden, Rechte der betroffenen Personen umgehen zu können. Auf der anderen Seite wird vertreten, im Sinne einer weiten Auslegung jede Form von Aufwendungen zu berücksichtigen. Nach dieser Lesart sollen sogar indirekte Folgekosten wie die Wartung der datenverarbeitenden Systeme vom Begriff der Implementierungskosten umfasst sein. Diese Auslegung wird damit begründet, dass nur so die Grundrechte des Verantwortlichen umfassend berücksichtigt werden könnten.[254] Dagegen spricht aber, dass der europäische Gesetzgeber zwischen den Kosten einer Maßnahme und den Implementierungskosten unterscheidet. So wurde noch in Art. 17 Abs. 1 der Datenschutzrichtlinie (95/46/EG) formuliert, dass Maßnahmen zur Datensicherheit u.a. die „bei ihrer Durchführung entstehenden Kosten“ berücksichtigen müssten. Daraus lässt sich schlussfolgern, dass der Begriff der Implementierungskosten in Art. 25 Abs. 1 DSGVO absichtlich gewählt wurde.[255]

Eine weitere noch nicht geklärte Frage ist, ob im Rahmen der Abwägung der angemessenen Mittel die beschränkte Wirtschaftskraft eines Verantwortlichen zu berücksichtigen ist. Dagegen spricht der Wortlaut von Art. 25 Abs. 1, der bezüglich der Implementierungskosten einen objektiven Maßstab nahelegt. Noch einschneidender ist aber das Argument, dass die mangelnde wirtschaftliche Leistungsfähigkeit in diesem Fall für den Verantwortlichen entlastend wirken und einen verminderten Schutz der Betroffenen rechtfertigen würde. In der Praxis könnte dies zur Folge haben, dass ein dem Risiko angemessener technischer Datenschutz nur bei umsatzstarken Großkonzernen zu erwarten ist. Dies würde den Regelungszweck von Art. 25 DSGVO konterkarieren.[256]

4.6 Datenschutzfreundliche Voreinstellungen

Der technische Datenschutz soll gemäß Art. 25 Abs. 2 DSGVO durch datenschutzfreundliche Voreinstellungen ergänzt werden, um sicherzustellen, dass nur für den jeweiligen bestimmten Verarbeitungszweck erforderliche Daten verarbeitet werden. Als Voreinstellungen werden Eingabevariablen bezeichnet, die den Betroffenen vom Verantwortlichen vorgegeben werden, bevor dieser das System zu nutzen beginnt.[257] Durch eine datenschutzfreundliche Gestaltung soll sowohl die Menge der erhobenen Daten als auch der Umfang ihrer Bearbeitung, ihre Speicherfrist und ihre Zugänglichkeit minimiert werden. Durch entsprechende Voreinstellungen ist außerdem sicherzustellen, dass Daten nicht unbeabsichtigt einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. Diesen Anforderungen liegt die Beobachtung zugrunde, dass werkseitig vorgegebene Voreinstellungen etwa infolge mangelnder Transparenz oder eines grundsätzlichen Vertrauens in die Hersteller

---

[254] *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 23.
[255] Martini in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 41.
[256] Vgl. *Schaffland/Holthaus* in: Schaffland/Wiltfang DS-GVO, Stand: 01.05.2017 Art. 25 Rn. 9; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 42; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 46.
[257] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 25 Rn. 47.

bzw. Anwender datenverarbeitender Systeme nur in seltenen Fällen verändert werden (sog. „Status Quo Bias“).[258]

Art. 25 Abs. 2 DSGVO soll den Grundsatz der Datenminimierung konkretisieren. Durch entsprechende Maßnahmen soll es den Betroffenen leichter gemacht werden, eigene Daten nur in dem Maß preiszugeben, das für den gewünschten Vorgang notwendig ist. Anders als beispielsweise Opt-Out-Lösungen, bei denen der Nutzer eine nicht erforderliche Datenverarbeitung manuell ausschalten muss, sollen Voreinstellungen gewährleisten, dass nur für den konkreten Zweck erforderliche Daten überhaupt erhoben und verarbeitet werden.

Nach Art. 25 Abs. 2 S. 2 DSGVO ist aber nicht nur die Datenmenge, sondern auch der Umfang ihrer Verarbeitung zu minimieren. Damit soll etwa eine Zusammenführung erhobener Daten zur Erstellung von Persönlichkeitsprofilen verhindert werden.[259] Trotz begrifflicher Überschneidungen mit dem Gebot der Datenminimierung ist diese Differenzierung wichtig, um auch die „Tiefe“ der Verarbeitung von für einen bestimmten Zweck notwendigerweise zu erhebenden Daten auf das erforderliche Maß zu reduzieren.[260] Nur so können zweckfremde Datenverarbeitungen effektiv zurückgedrängt werden. Auch die Beschränkung der Speicherfristen und der Zugänglichkeit der personenbezogenen Daten soll Missbrauchsmöglichkeiten durch den Verantwortlichen oder Dritte präventiv eindämmen und damit das Vertrauen in die Datenverarbeitung stärken.

Ebenso wie der Datenschutz durch Technikgestaltung ist auch der Grundsatz der Datenminimierung durch Voreinstellungen nicht als starre Verpflichtung zu verstehen. Sie stellt vielmehr eine legislative Vorgabe für die risikobasierte Abwägung des Datenschutzes mit den widerstreitenden Interessen der verschiedenen Beteiligten dar.[261] Regelungszweck ist es, die wirtschaftlichen Interessen der Verantwortlichen an einer möglichst umfassenden Datenverarbeitung dem Prinzip der Erforderlichkeit zu unterstellen.[262] Dennoch zeigen schon die wirtschaftlichen Grundrechte der Verantwortlichen aus Art. 15 Abs. 1 und Art. 16 GRCh, dass diese Priorisierung nicht grenzenlos gilt.[263] Auch wenn Art. 25 Abs. 2 DSGVO bei der Festlegung der gebotenen Voreinstellungen nicht explizit eine Berücksichtigung des Risikos einer Datenverarbeitung anordnet, dürfte auch in diesem Bereich ein risikobasierter Ansatz interessengerecht sein.[264] Schließlich ist zu beachten, dass es dem Betroffenen aufgrund seines Selbstbestimmungsrechts unbenommen bleiben muss, diese datenschutzfreundlichen Voreinstellungen nachträglich zu ändern oder aufzuheben.[265]

---

[258] Vgl. *Baumgartner/Gausling* ZD 2017, 308, 312; *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 14; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 63; *Wolff* in: Schantz/Wolff, 1. Auflage 2017, DSGVO, Rn. 838.

[259] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 50.

[260] *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 68.

[261] Vgl. *Plath,* in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 24 Rn. 2; *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 15.

[262] *Baumgartner/Gausling* ZD 2017, 308 (313).

[263] *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 21; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 25 Rn. 46.

[264] *Baumgartner/Gausling* ZD 2017, 308 (313).

[265] *Schaffland/Holthaus*, in: Schaffland/Wiltfang DS-GVO, Stand: 01.05.2017, Art. 25 Rn. 11.

4.7 Selbstregulierung

Die abstrakte Formulierung von Art. 25 Abs. 1 und 2 DSGVO ermöglicht es den Verantwortlichen, neue technologische Entwicklungen datenschutzrechtlich fruchtbar zu machen. Damit einhergehenden Unsicherheiten in der Rechtsanwendung soll nach dem Willen des europäische Gesetzgeber dadurch Rechnung getragen werden, dass gem. Art. 25 Abs. 3 DSGVO die Verantwortlichen zum Nachweis durch ein genehmigtes Zertifizierungsverfahren gemäß Art. 42 DSGVO als erbringen können.[266] Eine solche Zertifizierung soll die Rechtmäßigkeit der Datenverarbeitung zwar nicht fingieren, aber eine entsprechende Indizwirkung entfalten.[267] Auch genehmigte Verhaltensregeln im Sinne des Art. 40 DSGVO, die beispielsweise von Branchenverbänden erlassen wurden, können ein wichtiges Indiz für die Einhaltung der Regeln des Technikdatenschutzes herangezogen werden.

4.8 Rechtsfolgen und Sanktionen

Verstöße gegen Art. 25 DSGVO sind nach Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt, wobei Geldstrafen von bis zu € 10 Mio. oder 2 % des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens verhängt werden können. Nicht zuletzt aufgrund dieser empfindlichen Sanktionsmöglichkeiten liegt ein effektiver Datenschutz, im Rahmen dessen schon bei der Entwicklung technologischer Systeme die Vereinbarkeit mit der DSGVO berücksichtigt wird, auch im Interesse der Verantwortlichen.[268] Dabei ist zu beachten, dass die der sachliche Anwendungsbereich nach Art. 2 Abs. 1 DSGVO eine Datenverarbeitung voraussetzt. Deshalb stellt lediglich die Inbetriebnahme bzw. Nutzung datenverarbeitender Systeme, die entgegen der Vorschriften aus Art. 25 DSGVO entwickelt wurden, einen solchen Verstoß dar.[269]

Zudem kann der Betroffene gemäß Art. 82 Abs. 1 DSGVO Ersatzansprüche geltend machen, wenn die Integration der technischen und organisatorischen Maßnahmen in die Verarbeitungsprozesse nicht den Anforderungen aus Art. 25 DSGVO genügt und der Betroffene infolge dessen einen Schaden erleidet. Sofern sich ein Verstoß gegen Art. 25 DSGVO feststellen lässt, ist ein Verschulden des Verantwortlichen i.S.v. Art. 82 Abs. 3 DSGVO bereits indiziert.[270] Zu Gunsten des Verantwortlichen ist aber haftungsbegrenzend zu berücksichtigen, dass die Anforderungen des technischen Datenschutzes nach Art. 25 Abs. 1 DSGVO unter dem Vorbehalt der Stands der Tech-

---

[266] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 3 und Rn. 53; eine Darstellung der Zertifizierungsmöglichkeiten nach der DSGVO findet sich bei *Schneider* in: Forgó/Helfrich/Schneider, 2. Auflage 2017, Betrieblicher Datenschutz, Teil II, Kap. 5 Rn. 57 ff.

[267] *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 19; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 53.

[268] Hinzu kommt, dass eine nachträgliche Änderung der Produkte häufig mit noch höheren Kosten verbunden wäre, Vgl. *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 2.

[269] *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 6; *Plath* in: Plath, BDSG/DSGVO, 2. Auflage 2016 Art. 25 Rn. 4.

[270] *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 77.

nik und der Implementierungskosten stehen, sodass Art. 82 DSGVO keinen umfassenden Rechtsgüterschutz gewährt.[271]

4.9 Instrumente des technischen Datenschutzes

4.9.1 Hintergrund

Im Gesetzgebungsverfahren zu Art. 25 DSGVO wurde vielfach kritisiert, dass unklar bliebe, welche konkreten Maßnahmen den Anforderungen des technischen Datenschutzes genügen würden.[272] Rechtstechnisch ist dieser Einwand besonders beachtlich, weil die mit dem offenen Wortlaut der Norm einhergehende Rechtsunsicherheit im Spannungsfeld zu den erheblichen Sanktionsmöglichkeiten der Aufsichtsbehörden steht. Dieses Problem wird dadurch verschärft, dass der technische strafbewerte Datenschutz in rechtlicher Hinsicht Neuland darstellt, sodass nicht auf eine bestehende Rechtspraxis zurückgegriffen werden kann.

In der Tat werden im Wortlaut von Art. 25 DSGVO ausdrücklich lediglich die Pseudonymisierung als Maßnahme und die Datenminimierung als Zielvorgabe genannt. Regelungszweck dieser abstrakten Normgestaltung ist zum einen, neue technische Möglichkeiten zu Gunsten des Datenschutzes berücksichtigen zu können. Zum anderen soll dadurch die aus Sicht des europäischen Gesetzgebers erforderliche risikobasierte Einzelfallbetrachtung des Verantwortlichen hinsichtlich der angemessenen Maßnahmen ermöglicht werden.

4.9.2 Normative Vorgaben

Bei näherer Betrachtung finden sich in der DSGVO aber doch einige Vorgaben zu den in Frage kommenden Instrumenten des technischen Datenschutzes. Da die Maßnahmen darauf ausgelegt sein sollen, die Datenschutzgrundsätze wirksam umzusetzen, wird hinsichtlich der Ziele zumindest indirekt auf Art. 5 Abs. 1 DSGVO verwiesen. Zudem enthält der Erwägungsgrund 78 DSGVO weitere Ausführungen zu geeigneten technischen und organisatorischen Maßnahmen. Hinzu kommt, dass zahlreiche Querbezüge zu Art. 32 Abs. 1 DSGVO bestehen.[273] Dieser verfolgt mit der Datensicherheit zwar einen anderen Regelungszweck. Nichtsdestotrotz stellen die dort genannten technischen und organisatorischen Maßnahmen ebenso Praxisbeispiele für den Anwendungsbereich von Art. 25 DSGVO dar. Dies gilt etwa für die Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)[274] oder die

---

[271] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 6; nach *Nolte/Werkmeister*, in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 33 sollen Schadensersatzansprüche bei einem Verstoß gegen Art. 25 DSGVO sogar ganz ausgeschlossen sein, weil ein solcher weder zur Rechtswidrigkeit einer Datenverarbeitung noch zur fehlenden Gewährung von Betroffenenrechten führe.

[272] Vgl. *Piltz* K&R 2016, 709 (710); *Sydow/Kring* ZD 2014, 273; *Geis* ZD 2013, 591 (594); *Plath* in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 25 Rn. 3; *Hartung* in: Kühling/Buchner DS-GVO, 1. Auflage 2017, Art. 25 Rn. 17.

[273] *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 10; Kühling/Buchner/*Hartung*, 1. Aufl., DSGVO Art. 25 Rn. 16; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 55.

[274] Zur Begriffsbestimmung der Verschlüsselung nach der DSGVO, s. 4.9.3.3.

regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO).[275]

Daneben kann auch auf andere bereits anerkannte Privacy Enhancing Technologies zurückgegriffen werden.[276] Diesbezüglich ist insbesondere auf die Berichte der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zu verweisen, die sich sowohl mit der systematischen Umsetzung von Privacy by Design im Allgemeinen[277] als auch in Bezug auf Big Data[278] beschäftigen. Es ist zudem zu erwarten, dass die Aufsichtsbehörden konkretere Orientierungshilfen für die praktische Umsetzung von Art. 25 DSGVO veröffentlichen werden. Bis dahin können Verantwortliche auch auf bereits vorhandene Standards zurückgreifen. Dazu zählen in Deutschland etwa die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik.[279] Schließlich sind die Verantwortlichen mit den Nachweismöglichkeiten nach Art. 25 Abs. 3 DSGVO jedenfalls langfristig selbst in der Lage, mehr Rechtsicherheit zu schaffen.

4.9.3 Anwendungsbeispiele

Daraus ergibt sich, dass sich zahlreiche bereits praktizierte technische und organisatorische Maßnahmen in die neuen normativen Vorgaben einfügen. Für welche Maßnahmen sich der Verantwortliche konkret entscheidet, soll dem Regelungskonzept von Art. 25 DSGVO nach das Ergebnis einer einzelfallbezogenen Abwägungsentscheidung hinsichtlich des Aufwands und der Effektivität sein. Deshalb dürfte den Verantwortlichen bei der Überprüfung der getroffenen Maßnahmen ein weiter Ermessenspielraum zugestanden werden.[280] Im Folgenden sollen konkrete Maßnahmen des technischen Datenschutzes aus der Praxis aufgezeigt und innerhalb der neuen Vorschriften der DSGVO rechtlich eingeordnet werden.

4.9.3.1 Anonymisierung

4.9.3.1.1 Begriffsbestimmung

Durch eine Anonymisierung werden Daten vollständig und unumkehrbar von ihrem Personenbezug entkoppelt. [281] Insgesamt setzt eine wirksame Anonymi-

---

[275] Solche Verfahren unterfallen den möglichen organisatorischen Maßnahmen, s. 4.9.3.6.

[276] *Baumgartner/Gausling* ZD 2017, 308 (311 f.); *Hartung* in: Kühling/Buchner DS-GVO, 1. Auflage 2017, Art. 25 Rn. 18; *Plath* in: Plath, BDSG/DSGVO, 2. Auflage 2016, Art. 25 Rn. 3.

[277] ENISA, Privacy and Data Protection by Design – from policy to engineering, Dezember 2014, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (zuletzt aufgerufen am 15.11.2017).

[278] ENISA, Privacy by Design in big Data, Dezember 2015, https://www.enisa.europa.eu/publications/big-data-protection (zuletzt aufgerufen am 15.11.2016).

[279] Diese IT-Grundschutz-Kataloge können eingesehen werden unter www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Download/download_node.html (zuletzt aufgerufen am 15.11.2017).

[280] *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 48; *Baumgartner* in: Ehmann/Selmayr, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 10.

[281] *Ernst* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG Art. 4 Rn. 48; Kilian/Heussen/Polenz, Stand: Februar 2017, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes 13. Teil Rn. 76.

sierungslösung somit voraus, dass es infolge der Technikgestaltung nicht mehr möglich ist, ursprünglich personenbezogenen Daten den Betroffenen zuzuordnen.[282] Damit ist die Anonymisierung im Vergleich zu anderen technischen Maßnahmen, wie etwa Pseudonymisierungen, besonders rechtsschutzintensiv.

In diesem Zusammenhang ist klärungsbedürftig, ob es für eine Anonymisierung i.S.d. DSGVO ausreicht, dass der Verantwortliche selbst die Daten den betroffenen Personen nicht mehr zurechnen kann. Darüber hinaus könnte nämlich gefordert werden, dass eine Re-Identifizierung durch niemanden mehr möglich ist.[283] Praktisch steht dahinter die Frage, ob sich der Verantwortliche Zusatzwissen eines Dritten, der den Personenbezug dadurch nach wie vor rückkoppeln kann, zurechnen lassen muss. Diese Fragestellung greift der Erwägungsgrund 26 DSGVO explizit auf: Danach sollen bei der Feststellung, ob eine natürliche Person identifizierbar bleibt, alle Mittel berücksichtigt werden, die von Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden. Dafür sollen objektive Faktoren wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand herangezogen werden. Zusammengefasst soll ein Zusatzwissen Dritter einer Anonymisierung also nur entgegenstehen, wenn dessen Einsatz nicht aus wirtschaftlichen Gründen unwahrscheinlich ist.[284]

4.9.3.1.2 Methoden der Anonymisierung

Voraussetzung einer Anonymisierung ist stets, dass die expliziten Identifikationsmerkmale personenbezogener Daten gelöscht werden.[285]

Sofern es trotzdem möglich ist, eine Person innerhalb eines Datensatzes aufgrund einer bestimmten Merkmalsausprägung zu identifizieren, kann es darüber hinaus erforderlich sein, den Gehalt eines Datensatzes durch sog. Aggregierungen von dem Zuordnungsmerkmal zu trennen. Dabei werden mehrere Datensätze derart zusammengefasst, dass eine Re-Identifizierung einzelner personenbezogener Daten innerhalb dieses Gruppendatensatzes ist nicht mehr möglich ist.[286] So kann es etwa angezeigt sein, das Geburtsdatum einer betroffenen Person mit einer allgemein gehaltenen Aussage, etwa dem Geburtsjahr oder einer Kategorie wie „Alter unter 20 Jahre“, zu ersetzen.[287]

Daneben kann eine Anonymisierung technisch auch durch eine sog. Datensynthese erzeugt werden. Bei einer solchen werden Daten mit den gleichen statistischen Ei-

---

[282] Nach der Definition des § 3 V BDSG reicht es aus, wenn die Zuordnung einen unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde, s. dazu *Dammann* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 200; *Kühling/Klar* NJW 2013, 3611 (3613).

[283] S. zu diesem Streit zwischen relativem und absolutem *Rücker/Brandt* in: Bräutigam/Rücker E-Commerce, 1. Auflage 2017, 3. Teil D Rn. 61 f.; *Kühling/Klar* NJW 2013, 3611 (3614 f).

[284] *Marnau* DuD 2016, 428 (430).

[285] Zu diesen Merkmalen sind etwa Namen, Anschriften, Personenkennzeichen und individuelle Kontonummern zu zählen, s. *Gola* in: Gola, DS-GVO, 1. Auflage 2017, Art. 4 Rn. 40; *Dammann* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014*,* § 3 Rn. 206.

[286] *Ernst* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 4 Rn. 49; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 57.

[287] Vgl. *Dammann* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 207.

genschaften wie bei den bereits vorhandenen künstlich erzeugt, um eine Rückkoppelungsmöglichkeit des Personenbezugs zu unterbinden.[288] Je mehr kontrollierte Zufallsfehler auf diese Weise generiert werden, desto stärker ist die Schutzwirkung für die betroffenen Personen.[289]

4.9.3.1.3 Praktische Relevanz

Anonymisierte Daten sind nicht mehr personenbezogen und unterfallen daher nicht dem sachlichen Anwendungsbereich von Art. 2 Abs. 1 DSGVO.[290] Weitere technische und organisatorische Maßnahmen nach Art. 25 DSGVO sind anschließend nicht mehr nötig. Da der Personenbezug aber etwa zur Nutzerauthentifizierung erforderlich ist, dürften Systeme, die lediglich anonymisierte Daten verarbeiten, den Ausnahmefall darstellen. In Teilbereichen dürften Anonymisierungskonzepte aber gerade wegen der möglichen Bußgelder nach Art. 83 Abs. 4 lit. a DSGVO und der bestehenden Rechtsunsicherheit in Bezug auf die konkreten Anforderungen aus Art. 25 DSGVO als besonders durchgreifendes Instrument der Technikgestaltung eine hohe praktische Relevanz haben.[291]

4.9.3.2 Pseudonymiserung

4.9.3.2.1 Begriffsbestimmung

Maßnahmen der Pseudonymisierung sind in Art. 4 Nr. 5 DSGVO legal definiert und zeichnen sich dadurch aus, dass die betroffenen Personen ohne einen besonderen, getrennt aufbewahrten Schlüssel nicht mehr identifizierbar sind.[292] Personenbezogenen Daten werden demnach im Rahmen einer Pseudonymisierung „unter falschem Namen“ gespeichert.[293] Im Gegensatz zu anonymisierten Daten gelten die Grundsätze des Datenschutzes nach der DSGVO für pseudonymisierte Daten nach wie vor, weil diese immer noch Informationen über jedenfalls identifizierbare natürliche Personen enthalten.

Erforderlich ist also, dass die vorhandenen Daten der jeweils betroffenen Person nur unter Hinzuziehung zusätzlicher Informationen zugeordnet werden können. Dieser für die Identifizierung erforderliche Schlüssel muss zwingend getrennt von den Daten aufbewahrt werden, um eine unbefugte Zusammenführung effektiv zu verhindern. Das bedeutet in praktischer Hinsicht, dass die pseudonymisierten Daten und die zur

---

[288] *Baumgartner/Gausling* ZD 2017, 308 (312); *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 61; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 29.

[289] *Dammann* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 209.

[290] Dies wird in Erwägungsgrund 26 DSGVO ausdrücklich bestätigt; s. auch *Gola* in: Gola, DS-GVO, 1. Auflage 2017, Art. 4 Rn. 40; *Rücker/Brandt* in: Bräutigam/Rücker E-Commerce, 1. Auflage 2017, 3. Teil D Rn. 61; *Schneider* in: Schneider Datenschutz nach der DSGVO, 1. Auflage 2017, Rn. 60; Kilian/Heussen/Polenz, Stand: Februar 2017, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes 13. Teil Rn. 77.

[291] Vgl. *Conrad* ZD 2016, 553, 554.

[292] Vgl. dazu auch Erwägungsgrund 26 S. 2; s. zur Pseudonymisierung nach der DSGVO auch *Rücker/Brandt* in: Bräutigam/Rücker E-Commerce, 1. Auflage 2017, 3. Teil D Rn. 68 f.

[293] Dies entspricht der etymologischen Herkunftsbedeutung von Pseudonym, s. *Ernst* in Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 4 Rn. 40; *Schild,* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, DSGVO Art. 4 Rn. 71; *Dammann* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 213.

Re-Identifikation erforderliche Zusatzinformation weder auf dem gleichen Rechner liegen noch über das gleiche Nutzerkonto zugänglich sein dürfen.[294]

4.9.3.2.2 Arten der Pseudonymisierung

Eine Pseudonymisierung kann auf verschiedene Arten erfolgen: Zum einen kann der Betroffene selbst ein Pseudonym erstellen, bevor seine Daten durch das System verarbeitet werden, etwa durch eine frei gewählte Benutzer-ID ohne Namensbezug. Dies schützt die Betroffenen im besonderen Maße, da nur diese in der Lage sind, ihre Identität nachträglich offenzulegen.[295] Andererseits besteht die Möglichkeit, dass das Pseudonym durch einen vertrauenswürdigen Dritten vergeben wird, der allein über die Zuordnungsregel verfügt und den Personenbezug nur zu definierten Zwecken aufdecken darf. Ein Beispiel für dieses Modell ist die Verwaltung eines pseudonymisierten Zertifikats durch eine dafür ausgewiesene Stelle nach dem Signaturgesetz.[296] Drittens kann auch der Verantwortliche selbst das Pseudonym verwalten. Dadurch wird der Betroffene allerdings nicht gegenüber dem Verwender des datenverarbeitenden Systems geschützt, da dieser über die Zuordnungsregel verfügt und die Daten daher trotz Pseudonyms personenbezogenen verwenden kann. Allerdings kann auf diese Weise der unbefugte Zugriff durch Dritte verhindert werden.[297]

4.9.3.2.3 Praktische Relevanz

Der europäische Gesetzgeber hat bei der datenschutzrechtlichen Technikgestaltung einen besonderen Schwerpunkt auf die Pseudonymisierung gelegt.[298]

Diese Schwerpunktsetzung auf eine möglichst schnellen Pseudonymisierung der Daten stellt einen Kompromiss zwischen den Interessen der an einer Datenverarbeitung Beteiligten dar: Auf der einen Seite bleibt eine Zusammenführung der Daten und des jeweiligen Personenbezugs möglich, was im Hinblick auf den Verarbeitungszweck erforderlich sein kann, etwa um den Betroffenen bei Vertragspflichtverletzungen zur Rechenschaft ziehen zu können. Andererseits ist es auch möglich, Daten mit demselben Pseudonym in dem Sinne miteinander zu verketten, dass ein umfassendes Profil unter diesem Pseudonym entsteht. Auf diese Weise kann der Betroffene etwa von einem datenverarbeitenden System wiedererkannt und

---

[294] *Ernst* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 43.

[295] *Schild,* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, DSGVO, Art. 4 Rn. 75; *Scholz* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 220a; s. zu den Arten der Pseudonymisierung im Allgemeinen auch *Rücker/Brandt* in: Bräutigam/Rücker E-Commerce, 1. Auflage 2017, 3. Teil D Rn. 65; *Klar/Kühling*, in: Kühling/Buchner DS-GVO BDSG, 1. Auflage 2018, Art. 4 Nr. 5 Rn. 8; Kilian/Heussen/Polenz, Stand Februar 2017, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes 13. Teil Rn. 80.

[296] *Schild,* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, DSGVO Art. 4 Rn. 75; *Scholz* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 220b.

[297] *Schild,* in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.05.2017, DSGVO Art. 4 Rn. 76; *Scholz* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 220c.

[298] *Marnau* DuD 2016, 428 (430); Paulus in: Wolff/Brink BeckOK Datenschutzrecht, 20. Edition, Stand: 01.02.2017, Art. 25 Rn. 5; *Rücker/Brandt* in: Bräutigam/Rücker E-Commerce, 1. Auflage 2017, 3. Teil D Rn. 68; zurückhaltender wird auch von einer „im Vergleich zur DSRL leicht gesteigerte[n] Bedeutung“ gesprochen, s. *Klar/Kühling*, in: Kühling/Buchner DS-GVO BDSG, 1. Auflage 2018, Art. 4 Nr. 5 Rn. 4.

damit autorisiert werden, ohne dafür seine Identität preisgeben zu müssen.[299] Hinzu kommt, dass eine Pseudonymisierung den Betroffenen bereits relativ wirksam vor Identitätsdiebstählen und Persönlichkeitsverletzungen im Allgemeinen schützt. Denn für Außenstehende wird die Nutzbarmachung dieser Daten durch die Pseudonymisierung erheblich erschwert.[300] Dies gilt allerdings nur, wenn die Pseudonymisierung mit einer entsprechend hohen Datensicherheit einhergeht und die Verantwortlichen die jeweiligen Schlüssel effektiv vor einem unbefugten Zugriff zu schützen im Stande sind.[301] Eine solche Aufhebung der Pseudonymisierung durch Dritte wird in Erwägungsgrund 75 DSGVO explizit als mögliches Risiko der Datenverarbeitung aufgeführt.

Insgesamt dürfte sich das Instrument der Pseudonymisierung anbieten, wenn es bei der Datenverarbeitung nicht auf die jederzeitige Kenntnis der Identität des Betroffenen ankommt.[302]

4.9.3.3 Verschlüsselung

Im Rahmen einer Verschlüsselung werden die Daten durch kryptografische Maßnahmen so verändert, dass sie nur mithilfe eines Schlüssels lesbar sind. So können Daten insbesondere während ihres Übertragungsvorgangs vor unberechtigtem Zugang Dritter geschützt werden.[303] Im Gegensatz zur Pseudonymisierung bleibt der Personenbezug hier aber grundsätzlich vollständig erhalten, sodass die Verschlüsselung im Vergleich wiederum eine weniger rechtsschutzintensive Maßnahme darstellt. Dennoch kann sie in einigen Fällen ausreichend sein, um den Anforderungen des Art. 25 DSGVO zu genügen.[304]

4.9.3.4 Transparenz

4.9.3.4.1 Benutzerfreundliche Eingabemaske

Daneben gewinnt gerade bei elektronischen Einwilligungserklärungen die übersichtliche und benutzergerechte Wahrnehmung von Mitteilungs- und Benachrichtigungspflichten eine besondere Bedeutung.[305] Sie ist in Erwägungsgrund 78 DSGVO explizit als Maßnahme des technischen Datenschutzes aufgeführt. Dies zeigt die Wechselbeziehung zwischen der Umsetzung der Betroffenenrechte und der Gewährleistung einer den Anforderungen des Art. 25 Abs. 1 DSGVO genügenden Technikgestaltung. Denn nur wenn der Betroffene ausführlich über die technischen und organisatorischen Maßnahmen, mit denen der Verantwortliche seinen Pflichten aus Art. 25 DSGVO nachkommen möchte, informiert wird, kann dieser in die Lage versetzt wer-

---

[299] Vgl. *Dammann* in*:* Simitis Bundesdatenschutzgesetz, 8. Auflage 2014, § 3 Rn. 216.
[300] Sydow/*Mantz*, 1. Aufl., DSGVO, Art. 25 Rn. 51.
[301] Vgl. *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 55.
[302] *Klar/Kühling*, in: Kühling/Buchner DS-GVO BDSG, 1. Auflage 2018 Art. 4 Nr. 5 Rn. 1.
[303] *Martini* in Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 32 Rn. 34; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 56.
[304] Zur Bedeutung der Verschlüsselung nach der Konzeption der DSGVO, s. *Marnau* DuD 2016, 428, 431.
[305] *Nolte/Werkmeister* in: Gola, DS-GVO, 1. Auflage 2017, Art. 25 Rn. 15; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 29.

den, die Datenverarbeitung zu überwachen.[306] Die bedienungsfreundliche Handhabe und die damit einhergehende einfache Ausübung von Betroffenenrechten kann insbesondere durch eine entsprechend übersichtliche Gestaltung der Eingabemasken, sog. Dashboards, erreicht werden.[307]

4.9.3.4.2 Elektronische Etikette

Ein weiteres Beispiel für eine transparente Technikgestaltung i.S.v. Art. 25 DSGVO ist die Verwendung elektronischer Etiketten, auch Tags genannt. Durch deren Einsatz wird der Zweckbindungsgrundsatz aus Art. 5 Abs. 1 lit. b DSGVO gefördert, indem die legitimierten Verarbeitungszwecke nach außen hin sichtbar gemacht werden. Infolge der dadurch geschaffenen Transparenz können sowohl die versehentliche zweckfremde Verarbeitung als auch die Missbrauchsgefahr durch Dritte eingedämmt werden.[308]

4.9.3.5 Nutzerauthentifizierung durch single-sign-on-services

Ein weiterer Bereich, der insbesondere wegen des Gebots der Datenminimierung eine entsprechende technische Gestaltung erfordert, ist der der Nutzerauthentifizierung. Im Rahmen sog. single-sign-on-services können die zur Authentifizierung notwendigen Nutzerdaten hinterlegt werden, sodass deren Eingabe nur bei der ersten Anmeldung erfolgen muss. Anschließend werden diese Daten bei jeder weiteren Anmeldung nur in dem Umfang bereitgestellt, der für die Überprüfung der Berechtigung erforderlich ist. Ein Beispiel dafür ist die Kontrolle, ob ein Student infolge seiner Fakultätszugehörigkeit berechtigt ist, in einer Online-Bibliothek auf bestimmte Inhalte zugreifen zu können. Für die Beantwortung dieser Frage kann ein single-sign-on-service auf einen zuvor erfolgten einmaligen Nachweis zurückgreifen, der immer wieder verwendet werden kann. So werden die für die Nutzung eines Systems erforderlichen Daten effektiv minimiert.[309]

4.9.3.6 Organisatorische Maßnahmen

Den von Art. 25 DSGVO geforderten organisatorischen Maßnahmen unterfallen solche, die die äußeren Rahmenbedingungen der Datenverarbeitung betreffen.[310] In diesem Sinne sollte der Verantwortliche etwa festlegen, die jeweiligen Verarbeitungsvorgänge zu protokollieren und die Wirksamkeit der datenschutzfreundlichen Technikgestaltung in regelmäßigen Abständen zu kontrollieren. Daneben könnten als organisatorischen Maßnahmen auch technische Fortbildungen für die Beschäftigten und besondere interne Benachrichtigungspflichten bestimmt werden.

---

[306] Auch die Überwachungsmöglichkeit der Datenverarbeitung durch den Betroffenen wird nämlich in Erwägungsgrund 78 DSGVO als eine geeignete Maßnahme i.S.v. Art. 25 DSGVO genannt, Vgl. dazu *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 53.

[307] *Hartung* in: Kühling/Buchner DS-GVO BDSG, 1. Auflage 2018 Art. 25 Rn. 16; Martini in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 32.

[308] Vgl. *Martin*i in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 30; Kühling/Buchner/*Hartung*, 1. Aufl., DSGVO Art. 25 Rn. 16; *Mantz* in: Sydow, 1. Auflage 2017, DSGVO, Art. 25 Rn. 58.

[309] Vgl. *Baumgartner/*Gausling ZD 2017, 308, 312; *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 31.

[310] *Martini* in: Paal/Pauly, 1. Auflage 2018, DS-GVO BDSG, Art. 25 Rn. 28.

5 Anwendungsbeispiele

Im Rahmen eines Workshops am 9. November 2017 wurden drei konkrete Anwendungsfälle präsentiert. Nachfolgend werden die oben gewonnenen rechtlichen Erkenntnisse anhand dieser konkreten Praxisbeispiele erläutert.

5.1 Unterstützung bei der Materialauslagerung/ Kommissionierung

5.1.1 Sachverhalt

Im ersten Anwendungsfall sollen Kommissionierungstätigkeiten durch den Einsatz adaptiver Assistenzsysteme unterstützt werden. Kommissionierung meint die Zusammenstellung verschiedener Produktteile aus einer vorhandenen Gesamtmenge. Im Rahmen von Produktionsprozessen werden Kommissionierungsaufträge in aller Regel manuell ausgeführt. In dem zu untersuchenden Beispielprozess erhält der Beschäftigte eine Auftragsliste mit Einzelteilen, die für den weiteren Fertigungsprozess benötigt werden. Der Beschäftigte liest sich die Liste durch und steuert die verschiedenen Lagerplätze nacheinander an. Die zusammenzustellenden Einzelteile werden in der beauftragten Anzahl aus den Aufbewahrungsbehältnissen entnommen und in einem Sammelbehälter platziert. Anschließend hakt der Beschäftigte das entnommene Teil auf der Auftragsliste ab. Ist die Liste vollständig abgearbeitet, unterzeichnet der Beschäftigte diese und stellt die Einzelteile an einem Übergabepunkt für die weitere Verarbeitung bereit. Die einzelnen Arbeitsschritte werden durch das Einscannen von Barcodes nachgehalten. Beginn und Ausführung der Kommissionierung werden jeweils durch Eingaben an einem Computerarbeitsplatz im SAP-System dokumentiert.

Durch ein adaptives Unterstützungssystem soll der beauftragte Beschäftigte durch kontextsensitive Bereitstellung relevanter Informationen bei der Kommissionierung unterstützt werden. Ziel ist es, den Prozess zeiteffizienter und weniger fehleranfällig zu gestalten und den ausführenden Beschäftigten physisch und kognitiv zu entlasten. Die Unterstützung erfolgt durch den Einsatz einer Datenbrille, mit der die in der Kommissionierung tätigen Lagerbeschäftigten ausgestattet werden.

Zu Beginn der Kommissionierung authentifiziert sich der Beschäftigte im SAP-System, um einen Kommissionierungsauftrag zu erhalten. Der Beschäftigte wird sodann anhand der im System hinterlegten Informationen zum nächsten Lagerplatz geführt. Der anzusteuernde Gang und das betroffene Regalfach werden über die Datenbrille angezeigt. Für die visuelle Unterstützung müssen die Standortdaten des Beschäftigten mit den im System hinterlegten Navigationsdaten abgeglichen werden. Über das System werden außerdem die einzelnen Arbeitsschritte automatisch dokumentiert. Der Beschäftigte muss die Ausführung somit nicht mehr manuell bestätigen.

5.1.2 Rechtliche Beurteilung

Im Rahmen der geschilderten Unterstützung der Kommissionierung bzw. der Materialausgabe werden personenbezogene Daten des Beschäftigten, der mit Unterstüt-

zung der Datenbrille die Kommissionierung vornimmt, erhoben und verarbeitet: der Beschäftigte authentifiziert sich regelmäßig mit seinem Namen oder einer identifizierbaren Beschäftigtenkennung. Die Datenbrille zeichnet anschließend seine Standortdaten und die einzelnen Arbeitsschritte auf, um ihm das jeweils anzusteuernde Material anzuzeigen. Die Arbeitsschritte werden automatisch dokumentiert, und damit Daten über die Qualität und Dauer der ausgeführten Arbeiten des jeweiligen Beschäftigten erhoben, gespeichert und ggf. für weitere Zwecke genutzt.

5.1.2.1 Einwilligung

Als Rechtsgrundlage für die Datenverarbeitung käme theoretisch die Einwilligung des Beschäftigten in Betracht. Wie oben allerdings aufgeführt[311], ist es fraglich, ob die Einwilligung in einem solchen Fall freiwillig erfolgt. Dies wäre dann zu bejahen, wenn der Beschäftigte auch die Möglichkeit hätte, die Kommissionierung ohne Einsatz der Datenbrille vorzunehmen. Wird aber die Materialausgabe vollständig auf den Einsatz von adaptiven Assistenzsystemen umgestellt, ist der Beschäftigte gezwungen, diese Datenbrille zu nutzen. Die Einwilligung in die Verarbeitung seiner personenbezogenen Daten wäre dann nicht freiwillig.

Hinzu kommt das praktische Problem, dass eine Einwilligung widerrufbar ist. Die auf der Grundlage einer Einwilligung erfolgte Anschaffung von Datenbrillen wäre hinfällig, wenn Beschäftigten ihre Einwilligung widerrufen und damit den weiteren Einsatz der Datenbrillen unmöglich machen würden.

Im Ergebnis wird daher die Einwilligung im Regelfall keine adäquate Rechtsgrundlage für den im Anwendungsbeispiel beschriebenen Einsatz von Datenbrillen darstellen.

5.1.2.2 Datenverarbeitung im Rahmen der Durchführung des Beschäftigenverhältnisses, § 26 BDSG-neu

Die Verarbeitung personenbezogener Beschäftigtendaten bei Einsatz der Datenbrillen zur Kommissionierung dient den Zwecken, den Prozess zeiteffizienter und weniger fehleranfällig zu gestalten und den ausführenden Beschäftigten physisch und kognitiv zu entlasten. Damit erfolgt die Datenverarbeitung im Rahmen der Durchführung des Beschäftigtenverhältnisses nach § 26 BDSG-neu.[312]

Die Verarbeitung personenbezogener Daten des Beschäftigten ist zulässig, wenn sie erforderlich ist, um die genannten Zwecke zu erreichen. Die mit dem Einsatz der Datenbrille einhergehende Verarbeitung der Daten stellt ein grundsätzlich geeignetes Mittel dar, um die Zwecke zu erreichen. Mit den erhobenen Beschäftigtendaten ist es möglich, dem Beschäftigten konkrete Anweisungen zu geben, welche Materialausgabe er als nächstes anzusteuern hat.

Fraglich ist jedoch, ob diese Ziele nicht auch durch weniger einschneidende Maßnahmen erreicht werden können. So ist zum Beispiel zu hinterfragen, ob es tatsächlich jeweils einer Anmeldung des Beschäftigten und damit der Offenlegung seiner

---

[311] Vgl. oben D.IV.
[312] Vgl. oben D.I.1.

Identität bedarf. Um dem jeweiligen Beschäftigten die nächsten Arbeitsschritte anzuzeigen, ist eine Anmeldung des Beschäftigten nicht erforderlich. Die Anweisungen könnten auch anonym an den Beschäftigten erfolgen, der die Datenbrille jeweils trägt. Allerdings kann eine persönliche Anmeldung aus anderen Gründen gerechtfertigt sein. In Betracht kommen hier beispielsweise Gründe der Betriebssicherheit – nur berechtigte Beschäftigte sollen die Datenbrille nutzen -, der Arbeitsüberwachung und -steuerung, der Weiterbildung der Beschäftigten aufgrund der gewonnen Daten usw. Diese Zwecke der Datenerhebung sind vor Einsatz der Datenbrillen im Einzelnen festzulegen, um zu ermitteln, welche Verarbeitungsschritte tatsächlich für die festgelegten Zwecke erforderlich sind.

Kommt man zu dem Ergebnis, dass der Zweck nicht mit anonymisierten Daten erreicht werden kann, so sind die Interessen des Arbeitgebers gegenüber denen des Beschäftigten abzuwägen. Dabei ist auch die Schwere des Eingriffs in das Persönlichkeitsrecht des Beschäftigten zu berücksichtigen. Soll bspw. eine persönliche Anmeldung des Beschäftigten vor Nutzung der Datenbrille verhindern, dass Unbefugte die Datenbrille nutzen, dürften die Sicherheitsinteressen des Arbeitgebers im Regelfall überwiegen, so dass das Interesse des Beschäftigten, dass der Arbeitgeber möglichst keine Daten von ihm verarbeitet, dahinter zurücktreten muss.

Entsprechende Festlegungen sind auch für die einzelnen Datenverarbeitungsvorgänge zu treffen: auch wenn die Erhebung der personenbezogenen Daten für die konkreten Arbeitsanweisungen erforderlich ist, so ist damit noch keine Aussage verbunden, ob diese Daten auch nach Ausführung der konkreten Arbeitsanweisung weiterhin gespeichert und ggf. weiterverarbeitet werden dürfen. Eine nicht nur vorübergehende Speicherung ist für die Erreichung des Zwecks, dem Beschäftigten eine konkrete Arbeitsanweisung zu geben, nicht erforderlich. Dennoch kann auch die nicht nur vorübergehende Speicherung zulässig sein, wenn mit dieser weitere legitime Zwecke verfolgt werden. Dies wäre bspw. der Fall, wenn anhand der Daten überprüft werden soll, ob die Arbeitsaufträge korrekt ausgeführt wurden. Auch können durch die weitere Verarbeitung der anhand der Datenbrillen gewonnenen Daten neue Erkenntnisgewinne im Hinblick auf die Betriebsorganisation bezweckt werden, die eine solche Datenverarbeitung rechtfertigen können.

Grundsätzlich zulässig wäre es auch, die Beschäftigten, die diese Datenbrillen nutzen, zu kontrollieren. Allerdings darf die Anwendung nicht zu einer lückenlosen Überwachung der Beschäftigten führen. Daher ist zu prüfen, ob bei der Nutzung der Daten zu Zwecken der weiteren Optimierung der Betriebsorganisation die mit den Datenbrillen erhobenen Daten ohne Erkenntnisverlust nicht auch in anonymisierter Form verwendet werden können. Sollen die Daten zur Beschäftigtenschulung genutzt werden, dürfen diese nur für diesen konkreten Zweck und nicht bspw. für eine Bewertung des Beschäftigten durch die Personalabteilung genutzt werden.

Im Ergebnis gilt somit, dass die Erhebung von personenbezogenen Daten des Beschäftigten im Rahmen der Nutzung der Datenbrillen für konkrete Arbeitsanweisungen im Rahmen des § 26 BDSG-neu zulässig ist. Jede weitere Verwendung der so gewonnen Daten, bspw. zur Beschäftigtenkontrolle, zur Betriebsoptimierung oder zur weiteren Erkenntnisgewinnung bedarf einer Abwägung im Einzelfall. Dabei sind die konkreten Zwecke festzulegen und mit dem Interesse der Beschäftigten, insb. im Hinblick darauf, keiner Dauerüberwachung und einer Profilbildung unterworfen zu sein, abzuwägen.

Eine solche Abwägung wird insbesondere dann erforderlich, wenn die Datenbrille nicht nur die Aufgabe der konkreten Assistenz erfüllen soll, sondern die erhobenen Daten mit Daten anderer Assistenzsysteme oder anderweitig im Betrieb erhobenen Daten vernetzt werden. Adaptive Assistenzsysteme zeichnen sich gerade dadurch aus, dass eine Vernetzung mit weitern Daten erfolgt und diese dann wiederum auch zur Verbesserung des konkreten Assistenzsystems genutzt werden. Eine solche Vernetzung wird in der Regel anonym erfolgen können, so dass eine Verarbeitung personenbezogener Daten nicht erforderlich ist. Sollen aber beispielsweise die mit der Datenbrille erhobenen personenbezogenen Daten mit Daten aus anderen Kommissionierungsvorgängen verarbeitet werden, um daraus Erkenntnisse für die Betriebsorganisation, Bestellvorgänge oder Beschäftigteneinsätze abzuleiten darf auch eine solche Datenverarbeitung nur unter Berücksichtigung der Interessen des jeweiligen Beschäftigten erfolgen.

5.2 Rüsten

5.2.1 Sachverhalt

In der Produktion bezeichnet Rüsten einen Arbeitsschritt, bei dem ein Betriebsmittel für den nächsten Produktionsabschnitt vorbereitet wird. In dem zu untersuchenden Beispielsprozess bestücken Beschäftigte im Rahmen der Elektronikfertigung Produktionsanlagen mit Bauteilrollen, auf denen eine Vielzahl von Kleinstbauteilen aufgereiht ist. Spezielle Fertigungsmaschinen spulen die Rollen nach und nach ab und entnehmen die jeweils benötigten Einzelteile. Ist eine Bauteilrolle aufgebraucht, wird dies dem Beschäftigten über einen zentralen Monitor in der Produktionshalle angezeigt (sog. Hitliste). Der Beschäftigte entnimmt die benötigte Bauteilrolle aus einem speziellen Lagersystem (Tower) und begibt sich zu der Produktionsanlage, für die auf der Hitliste ein Materialbedarf angezeigt wird. Der Rollenwechsel erfolgt mithilfe einer speziellen Vorrichtung (sog. Feeder). Da jeder Feeder eine Vielzahl von unterschiedlichen Bauteilrollen enthält, besteht eine Herausforderung für den Beschäftigten darin, die nachzurüstende Rolle und die richtige Spur zu erkennen. Zur Überprüfung scannt der Beschäftigte über einen Handscanner nacheinander spezielle Barcodes auf der nachgefüllten Spur, der alten sowie der neuen Rolle.

Der Prozess soll durch den Einsatz eines adaptiven Assistenzsystems in Form einer Smartwatch sowie einer Datenbrille unterstützt werden. Dem Beschäftigten werden die Hitliste und der als nächstes auszuführende Auftrag direkt über das mitgeführte System angezeigt. Die Notwendigkeit, den zentralen Monitor ständig im Auge zu behalten, entfällt. Die Datenbrille unterstützt zudem die Navigation des Beschäftigten, indem sie den Tower mit dem jeweils benötigten Material farblich markiert. Beim Wechsel der Rollen wird außerdem die auszutauschende Rolle über die Brille durch eine farbliche Überlagerung sichtbar gemacht. Im System werden die einzelnen Arbeitsschritte nachgehalten. Zum Zwecke der Qualitätssicherung wird dabei auch erfasst, welcher Beschäftigte die Arbeitsschritte durchführt.

5.2.2 Rechtliche Beurteilung

Auch bei diesem Anwendungsfall ist geplant, personenbezogene Daten des Beschäftigten, der mit Unterstützung einer Smartwatch und einer Datenbrille die Arbeiten ausführt, zu erheben und zu verarbeiten: Die Instrumente geben dem Beschäftigten

konkrete Arbeitsanweisungen und zeichnen im Gegenzug die jeweils ausgeführten Arbeitsschritte auf. Die Arbeitsschritte werden anschließend dokumentiert und ausgewertet, um die Qualität der ausgeführten Arbeiten zu kontrollieren.

5.2.2.1 Einwilligung

Als Rechtsgrundlage für die Datenverarbeitung käme theoretisch die Einwilligung des Beschäftigten in Betracht. Hier gilt allerdings das zur Datenbrille Ausgeführte: Der Beschäftigte wird im Regelfall keine Wahl haben, ob er die Arbeit mit oder ohne die adaptiven Assistenzsysteme ausführen will. Er hat somit keinen Einfluss darauf, ob seine personenbezogenen Daten verarbeitet werden oder nicht. Auch wenn die Assistenzsysteme dem Beschäftigten wesentliche Vorteile bieten, weil sie ihm die Arbeitsschritte anzeigen und er nicht mehr auf den Bildschirm schauen muss, kann keine Freiwilligkeit unterstellt werden. Gerade weil die Erhebung und Verarbeitung auch seiner personenbezogenen Daten Rückschlüsse auf die Durchführung der Arbeitsschritte und damit auf die Qualität und Geschwindigkeit seiner Arbeitsleistung, ggf. auch im Vergleich zu anderen Beschäftigten, geben, erfolgt eine Einwilligung im Regelfall nicht freiwillig. Das Persönlichkeitsrecht gebietet es, dass der Beschäftigte selbst entscheiden kann, ob für ihn die Vorteile durch Nutzung eines Assistenzsystems die Nachteile durch Aufzeichnung seines Arbeitsverhaltens überwiegen.

Auch wenn man dem Beschäftigten die Entscheidung überlassen würde, ob er eine Arbeit ausführt, bei der eine Datenverarbeitung durch Nutzung adaptiver Assistenzsysteme erfolgt, oder lieber einen anderen Arbeitsplatz im Betrieb übernimmt, wird es im Regelfall an der Freiwilligkeit fehlen. Nur wenn die Arbeitsplätze gleichwertig sind und keine Nachteile für den Beschäftigten mit sich bringen, kann von einer freiwilligen Einwilligung gesprochen werden. Aber auch in diesem Fall bestünde weiterhin das Problem der Widerrufbarkeit der Einwilligung.[313]

Im Ergebnis wird daher die Einwilligung im Regelfall auch beim Rüsten keine adäquate Rechtsgrundlage für den Einsatz der adaptiven Assistenzsysteme bieten.

5.2.2.2 Datenverarbeitung im Rahmen der Durchführung des Beschäftigtenverhältnisses, § 26 BDSG-neu

Auch beim Rüsten steht der Zweck der Arbeitserleichterung und der Fehlervermeidung im Vordergrund. Indem der Beschäftigte die Informationen über eine Smartwatch bzw. eine Datenbrille „mit sich führt“, muss er nicht einen zentralen Monitor beobachten. Die „Hitliste“ wird dem Beschäftigten angezeigt, der diese nächsten Arbeitsschritte ausführen soll. Ein zentraler von allen Beschäftigten einsehbarer Monitor entfällt. Zudem wird dem Beschäftigten die Navigation im Betrieb erleichtert, da ihm die Stelle, an der er die Spule entnehmen muss, angezeigt wird. Über die Datenbrille wird kontrolliert, ob die richtige Spule eingelegt wird. Die Verarbeitung von personenbezogenen Daten erfolgt anlässlich der konkreten Durchführung der dem Beschäftigten obliegenden Tätigkeit, somit im Rahmen der Durchführung des Beschäftigtenverhältnisses nach § 26 BDSG-neu.[314]

---

[313] Vgl. oben D.IV.3.
[314] vgl. oben D.I.1.

Die Verarbeitung personenbezogener Daten des Beschäftigten ist zulässig, wenn sie erforderlich ist, um die genannten Zwecke zu erreichen. Die personenbezogenen Daten des Beschäftigten werden erhoben und genutzt, um die Durchführung der Arbeit zu erleichtern und die Qualität zu sichern. Die Datenverarbeitung stellt dabei ein geeignetes Mittel dar, um diese Ziele zu erreichen. Denn mit den konkreten Standortdaten des Beschäftigten kann das anzusteuernde Ziel angegeben werden. Die Angaben zur entnommenen Rolle ermöglichen einen Vergleich zur benötigten Rolle. Die Anzeige der Hitliste ermöglicht die Planung der nächsten Arbeitsschritte. Anhand der Beschäftigtendaten kann geprüft werden, ob der Beschäftigte die vorgegebenen Arbeitsschritte fehlerfrei und in angemessener Zeit ausgeführt hat. Damit stellt die mit den Assistenzsystemen einhergehende Datenverarbeitung auch hier ein geeignetes Mittel zur Erreichung der angestrebten Ziele dar.

Als nächster Schritt ist auch hier zu prüfen, ob diese Ziele nicht auch durch weniger einschneidende Maßnahmen erreicht werden können. Die Anzeige der Hitliste beispielsweise erfolgte bisher auf einem zentralen Monitor. Dieser Monitor wird nun durch eine Smartwatch des Beschäftigten ersetzt. Soweit es lediglich um die Anzeige der Hitliste geht, ist eine Anmeldung des Beschäftigten, und damit eine Erhebung seiner personenbezogenen Daten, nicht erforderlich. Wie der zentrale Monitor wäre es denkbar, dass auch die Smartwatch dem jeweiligen Träger die Hitliste anzeigt, ohne dass der Beschäftigte jeweils identifiziert wird.

Allerdings soll die Anzeige der Hitliste auf der Smartwatch auch ermöglichen, individualisierte Arbeitsschritte vorzugeben. So wird ein zentraler Monitor möglicherweise von mehreren Beschäftigten zur Bestimmung der nächsten durchzuführenden Arbeitsschritte genutzt. Die Smartwatch dagegen könnte hier auch Arbeitsverteilungsaufgaben übernehmen, die aber eine Individualisierung der Beschäftigte voraussetzt. Denn nur so kann sichergestellt werden, dass eine Arbeitsaufgabe einer bestimmten Person zugeordnet wird. In diesem Fall ist die Verarbeitung personenbezogener Daten auch erforderlich.

Die Navigation anhand der Smartwatch und die Anzeige der richtigen Spule in der Datenbrille könnten grundsätzlich ebenfalls anonym für den jeweiligen Träger erfolgen. Die Ziele der Arbeitserleichterung und der Effizienzgewinnung lassen sich auch ohne Verarbeitung von Beschäftigtendaten erreichen. Ein weiteres Ziel der Datenverarbeitung besteht jedoch in der Qualitätssicherung. Es soll gerade überprüft werden, ob der ausführende Beschäftigte die Aufgaben fachgerecht und in angemessener Zeit ausführt. Diese Ziele können nur erreicht werden, wenn Beschäftigtendaten erfasst werden.

In einem weiteren Schritt ist zu prüfen, ob die Datenverarbeitung auch verhältnismäßig ist. Die Interessen des Arbeitgebers an der Qualitätssicherung sind also gegenüber den Interessen des Beschäftigten abzuwägen. Das Interesse des Arbeitgebers, bei Einsatz der Assistenzsysteme zu kontrollieren, ob die Arbeitsschritte vom jeweiligen Beschäftigten entsprechend der Anweisungen ausgeführt werden, wird im Regelfall überwiegen. Denn nur bei Identifizierung des Beschäftigten ist es möglich, auf Fehler und Ineffizienzen beispielsweise durch Schulungsmaßnahmen oder durch Veränderung der Arbeitsabläufe zu reagieren. Wird der Beschäftigte identifiziert, werden folglich auch Daten zu seinem Standort und zu seinem Arbeitsveralten erhoben und genutzt. Das Interesse des Beschäftigten daran, dass möglichst wenige Daten von ihm erhoben werden, wird regelmäßig dahinter zurückstehen müssen.

Denn auch der Beschäftigte hat ein Interesse am Einsatz der Assistenzsysteme, da sie die Ausführung des Rüstens erleichtern. Der Eingriff in das Persönlichkeitsrecht des Beschäftigten ist relativ gering. Der Arbeitgeber darf daher im Rahmen seines ihm zustehenden unternehmerischen Ermessens die Anwendung der Smartwatch und der Datenbrille anordnen.

Eine Grenze wäre jedoch dann erreicht, wenn die Arbeitsschritte und das Arbeitsverhalten über den ganzen Arbeitstag hinweg aufgezeichnet und verarbeitet würde. Das wäre bspw. der Fall, wenn der Beschäftigte die Smartwatch zu Arbeitsbeginn anzieht und diese dann über den ganzen Tag, also z.B. auch während der Pausen, Standort und Tätigkeit aufzeichnet. Eine solche umfassende Personenkontrolle wäre auch zur Verfolgung der genannten Ziele nicht erforderlich. Es muss daher sichergestellt werden, dass die Smartwatch bzw. die Datenbrille nur den jeweiligen Arbeitsschritt, für den sie benötigt wird, aufzeichnet. Die Smartwatch könnte sich beispielsweise einschalten, wenn die Hitliste abgerufen werden soll. Standortdaten werden ausschließlich dann aufgezeichnet, wenn die Smartwatch Navigationsdaten weitergibt. Es ist zudem regelmäßig zu überprüfen, ob die personenbezogenen Daten für den jeweiligen Zweck noch erforderlich sind oder ob die Assistenzsysteme – ggf. nach einer Einführungsphase – auch mit anonymen Daten ihre Unterstützungsfunktion erfüllen können.

5.3 Sichtprüfen und Verpacken

5.3.1 Sachverhalt

Im Rahmen eines ebenfalls untersuchten Anwendungsfalls werden Beschäftigte an einem Trainingsarbeitsplatz auf einen komplexen Montage- und Verpackungsprozess vorbereitet. Eine solche Vorbereitung kann etwa beim Anlernen neuer Beschäftigter oder nach Einführung eines neuen Produkttyps erforderlich sein. Zu Beginn des Prozesses loggt sich der Beschäftigte im System ein. Anschließend scannt der Beschäftigte den Barcode des Produkts per Hand. Sodann werden dem Beschäftigten die Arbeitsschritte über einen stationären Computerbildschirm nacheinander angezeigt. Der Beschäftigte folgt den Anweisungen und bestätigt jeden ausgeführten Arbeitsschritt durch Mausklick. Der Ablauf im Trainingsmodus ist im Vergleich zum Produktivsystem deutlich verlangsamt. Der permanent erforderliche Abgleich von Arbeitsprodukt und Bildschirmanweisung und die Bedienung per Maus führen zu einer ständig wechselnden Verlagerung des Aufmerksamkeitsschwerpunkts.

Durch Einbindung adaptiver Assistenzsysteme soll der Arbeitsablauf einfacher und zeiteffizienter gestaltet werden. Der anzulernende Beschäftigte wird mit einer Datenbrille ausgestattet, die ihn in die Lage versetzt, den gesamten Arbeitsablauf freihändig zu steuern. Über die Datenbrille wird der Barcode des Produkts gescannt. Auch die Anweisungen zu den einzelnen Arbeitsschritten erhält der Beschäftigte direkt über die Datenbrille. Er kann sich so während des gesamten Prozesses auf die jeweils durchzuführenden Arbeitsschritte fokussieren und muss den Blick nicht mehr ständig auf den Bildschirm richten. Auch die einzelnen Prüfmerkmale werden über die Datenbrille direkt am Produkt angezeigt. Zusätzlich ermöglichen Bewegungssensoren eine Steuerung des Systems über Handgesten. Der Beschäftigte kann so ohne Betätigung eines Eingabegeräts jeden absolvierten Arbeitsschritt bestätigen

und die nächste Sequenz einleiten. Die Anmeldung zum System erfolgt personalisiert über WLAN oder Nahfeldkommunikation (Near Field Communication, kurz NFC).

5.3.2 Rechtliche Würdigung

5.3.2.1 Einwilligung

Bei diesem Anwendungsfall könnte auch die Einwilligung in Betracht kommen, wenn das Üben am Arbeitsplatz dem Beschäftigten freigestellt ist. Die Verarbeitung von personenbezogenen Daten an diesem Arbeitsplatz ist per se nur vorübergehend. Neue Beschäftigte sollen lernen, wie die Arbeitsschritte später auszuführen sind. Ihnen wird die Gelegenheit eröffnet, vor „Real-time-Einsatz“ die Arbeiten probeweise mit Anweisungen in einem verlangsamten Rhythmus auszuführen. Die vorhandene Belegschaft soll mit diesem Gerät neue Produktionsschritte lernen. Es ist denkbar, dass dem Beschäftigten die für ihn jeweils neuen Arbeitsschritte erläutert werden, und es ihm dann freisteht, diese zuvor an dem Arbeitsplatz zu üben. Ebenso hat in einigen Anwendungsfällen ein Beschäftigter die Möglichkeit, Arbeitsschritte, deren Ablauf er nicht mehr sicher kennt, beispielsweise nach einem Urlaub oder einem anderen Arbeitseinsatz, für sich erneut zu üben. Bei all diesen Anwendungen ist das Üben freigestellt. In diesen Fällen ist es ohne weiteres möglich, von dem Beschäftigten vor Nutzung dieses Übungsplatzes eine Einwilligung in die Verarbeitung seiner personenbezogenen Daten einzuholen. Allerdings sollten dem Beschäftigten dadurch, dass er diesen Arbeitsplatz nicht nutzt, keine Nachteile entstehen. Es muss also möglich sein, die neuen Arbeitsschritte auch auf andere Weise zu erlernen.

Ein Widerruf der Einwilligung gilt immer nur für die Zukunft. Für den vorliegenden Anwendungsfall bedeutet dies, dass der betroffene Beschäftigte ab diesem Zeitpunkt den Arbeitsplatz nicht mehr benutzen darf – oder jedenfalls nicht mehr auf der Grundlage einer Einwilligung.

5.3.2.2 § 26 BDSG-neu

Für diesen Anwendungsfall ist die Rechtfertigung über § 26 BDSG-neu evident. Zwar würde die Methode des Übungsarbeitsplatzes grundsätzlich auch anonym funktionieren. Die Übung soll aber im Regelfall dem Arbeitgeber und/oder dem Beschäftigten Aufschluss darüber geben, ob ausreichend Kenntnisse für einen Einsatz in der Produktion vorhanden sind. Auch sollen Lernfortschritte der Beschäftigte registriert werden, um die Arbeitsschritte in der Produktion entsprechend anpassen zu können. Das Interesse des Arbeitgebers, diese Ziele mithilfe der Verarbeitung von Beschäftigtendaten zu verfolgen, überwiegt. Der Beschäftigte hat kein oder nur ein untergeordnetes Interesse daran, dass sein Daten bei Nutzung dieses Übungsfalls nicht verarbeitet werden.

5.4 Kollektivvereinbarung als Rechtfertigungsgrundlage zur Datenverarbeitung bei den Anwendungsfällen

Als Rechtsgrundlage für alle drei Anwendungsbeispiele käme auch die Kollektivvereinbarung in Betracht. Den Adaptivsystemen in den genannten Anwendungsbeispielen kommt keine (oder nur eine untergeordnete) Kontrollfunktion zu, so dass ein Mit-

bestimmungsrecht nicht anzunehmen ist. Dennoch erscheint eine Kollektivvereinbarung bei Einführung der Systeme zweckmäßig.

In einer solchen Kollektivvereinbarung kann konkret festgelegt werden, wie die Assistenzsysteme funktionieren und welche Beschäftigtendaten zu welchen Zwecken erhoben und verarbeitet werden. Durch konkrete Regelungen können so Rechtsunsicherheiten erheblich reduziert werden. Für die Arbeitgeber hat dies den Vorteil, auf diese Weise auch ihre Transparenzpflichten zu erfüllen.[315]

[315] Vgl. oben E.II.3.

Anhang

A1 Muster für eine Betriebsvereinbarung

Betriebsvereinbarung zum Einsatz eines adaptiven Arbeitsassistenzsystems

Zwischen

des Unternehmens X [**Anm.:** *Name und Anschrift ergänzen*],

– nachfolgend Arbeitgeber genannt –

und

dem Betriebsrat der X,

– nachfolgend Betriebsrat genannt –

wird folgende Vereinbarung getroffen:

Präambel

Die Parteien sind sich einig, dass durch den Einsatz adaptiver Arbeitsassistenzsysteme Arbeitsabläufe unterstützt werden können. Gleichzeitig kann der Einsatz solcher Systeme in die Persönlichkeitsrechte der Beschäftigten eingreifen. Daher soll diese Betriebsvereinbarung den Einsatz des in Anlage 1 beschriebenen adaptiven Assistenzsystems regeln und dabei die Persönlichkeitsrechte der betroffenen Beschäftigten unter Berücksichtigung der gesetzlichen Vorgaben sichern.

§ 1

Regelungsgegenstand

(1) Gegenstand der Vereinbarung ist die Einführung und Nutzung eines adaptiven Assistenzsystems zur [**Anm.:** Hier sollte das Systems kurz beschrieben werden. Etwa: „Gegenstand der der Vereinbarung ist die Einführung und Nutzung eines adaptiven Assistenzsystems zur Unterstützung von Kommissionierungstätigkeiten [...].“] (nachfolgend „**System**“) sowie die damit verbundene Verarbeitung personenbezogener Daten im Sinne der DSGVO durch den Arbeitgeber. Eine Beschreibung des Systems ist dieser

Vereinbarung als Anlage 1 beigefügt. [**Anm.:** In der Anlage sollte die eingesetzte Hard- und Software überblicksartig beschrieben werden.]

(2) Soweit nichts anderes bestimmt ist, finden in dieser Vereinbarung die Begriffsbestimmungen der DSGVO Anwendung.

§ 2

Geltungsbereich

(1) Die Betriebsvereinbarung erstreckt sich auf alle Arbeitnehmerinnen und Arbeitnehmer des Arbeitgebers im Sinne des § 5 BetrVG (nachfolgend „**Beschäftigte**“).

(2) Die Betriebsvereinbarung gilt für alle Betriebsstätten des Arbeitgebers.

§ 3

Zweck und Funktion des Systems

(1) Das System soll [**Anm.:** Hier sollte Zweck und Funktionsweise des Systems kurz beschrieben werden. Etwa: *„Das System soll die Kommissionierungstätigkeit der Beschäftigten durch die Bereitstellung kontextsensitiver Informationen unterstützen. Die Beschäftigten werden hierzu mit Datenbrillen ausgestattet, über die sie sich den auszuführenden Auftrag anzeigen lassen und einen Abgleich der zusammengestellten Einzelteile mit der Auftragsliste vornehmen können. Das System erfasst den Standort des Beschäftigten und navigiert ihn zum anzusteuernden Lagerplatz.* [...]].

(2) Das System enthält Schnittstellen zu den in Anlage 2 beschriebenen Drittsystemen und Programmen. Ein Export und die Weiterverarbeitung von Beschäftigtendaten in andere Programme dürfen nur zu den in Abs. 1 beschriebenen Zwecken erfolgen.

(3) Die Parteien stellen klar, dass das System nicht zum Zwecke der Arbeitnehmerüberwachung oder der Leistungskontrolle eingesetzt werden darf.

§ 4

Beschäftigtendaten als Gegenstand der Verarbeitung

(1) Über das System werden ausschließlich die folgenden Daten erfasst und verarbeitet:

[**Anm.:** Hier sollten die im Rahmen des Systems verarbeiteten personenbezogenen Daten der Beschäftigten aufgelistet werden. Etwa:

- *„Mitarbeiterkennung des Beschäftigten*
- *Standort*
- *Login- und Logout-Zeitpunkt*
- *Standort*
- *Arbeitsschritt und Bearbeitungsstand des auszuführenden Auftrags*
- *[...]“]*

(2) Die erfassten Daten werden in Protokolldateien dokumentiert.

§ 5

Datenspeicherung und Löschung

(1) Der Arbeitgeber darf auf Grundlage der Protokolldateien Statistiken zum Zweck der Qualitätskontrolle erstellen. Informationen dürfen dabei nur anonymisiert erfasst werden und keinen Rückschluss auf einzelne Beschäftigte ermöglichen.

(2) Protokolldateien werden spätestens nach einer Woche gelöscht, sofern gesetzliche Regelungen nicht ausnahmsweise eine längere Speicherung erfordern.

§ 6

Schulung und Information der Beschäftigten

(1) Der Arbeitgeber informiert alle betroffenen Beschäftigten in geeigneter Weise über die Einführung des Systems. Die Beschäftigten werden in diesem Zusammenhang über Art und Umfang der verarbeiteten Daten in Kenntnis gesetzt.

(2) Die betroffenen Beschäftigten erhalten vor Inbetriebnahme des Systems bzw. bei Arbeitsaufnahme eine Einweisung in das System in Form einer kurzen Schulung. Jeder Beschäftigte erhält eine Bedienungsanleitung.

§ 7

Kontrollrechte des Betriebsrats

(1) Der Betriebsrat kann die Einhaltung dieser Betriebsvereinbarung jederzeit kontrollieren und dabei im Beisein einer fachkundigen, von dem Arbeitgeber zu benennenden Person in Programme, Dateien und Berichte Einsicht nehmen. Er hat dabei die Persönlichkeitsrechte der Beschäftigten zu wahren.

(2) Der Betriebsrat hat das Recht, einen Sachverständigen zur Kontrolle dieser Vereinbarung hinzuzuziehen.

(3) Weitere Rechte des Betriebsrats gem. BetrVG werden durch diese Vereinbarung nicht eingeschränkt

§ 8

Schlussbestimmungen

(1) Diese Betriebsvereinbarung tritt am [...] in Kraft. Sie kann jeweils zum Ende eines Jahres mit einer Frist von [...] Monaten gekündigt werden, frühestens jedoch zum [...].

(2) Sollten einzelne Punkte dieser Betriebsvereinbarung ungültig sein oder ihre Gültigkeit aufgrund neuer Gesetzgebung oder Rechtsprechung verlieren, so bleiben die übrigen Bestimmungen hiervon unberührt. In diesem Fall werden die Parteien unverzüglich über eine Ergänzung dieser Betriebsvereinbarung beraten.

A2 Checkliste zur Prüfung der datenschutzrechtlichen Zulässigkeit eines adaptiven Arbeitsassistenzsystems

Soweit beim Einsatz von adaptiven Arbeitsassistenzsystemen im Unternehmen Beschäftigtendaten verarbeitet werden, sind die datenschutzrechtlichen Vorgaben, insb. aus dem neuen Bundesdatenschutzgesetz (BDSG-neu) und der Datenschutzgrundverordnung (DSGVO), die überall in der Europäischen Union unmittelbar anwendbar ist, zu beachten. Beide Vorschriften treten am 25. Mai 2018 in Kraft. Die nachfolgende Checkliste soll einen kurzen Überblick über einige wichtige Regelungen geben, die zu beachten sind. Sie ist weder vollständig, noch kann sie im Einzelfall eine Beratung ersetzen. Sie kann lediglich dazu dienen, das Problembewusstsein zu schärfen und einen ersten Anhaltspunkt liefern, ob weitere Maßnahmen oder eine Beratung erforderlich sind.

I. Anwendbarkeit des Datenschutzrechts

Das Datenschutzrecht ist nur anwendbar, wenn die verarbeiteten Daten Personenbezug aufweisen:

Werden Daten von Beschäftigen (Arbeitnehmer und Arbeitnehmerinnen, freie Mitarbeiterinnen und Mitarbeiter) verarbeitet, bspw. weil sich der Beschäftigte vor Nutzung des Systems anmeldet oder das Arbeitsassistenzsystem einem bestimmten Beschäftigten zugeordnet ist? ☐

Falls eine unmittelbare Identifizierung nicht erfolgt, ist es aufgrund der erhobenen Daten möglich, den Beschäftigten zu identifizieren, bspw. aufgrund von Einsatzplänen oder anderen persönlichen Merkmalen (Fotos, Video, IP-Adresse)? ☐

> Nur wenn ausschließlich anonyme Daten verarbeitet werden, ist das Datenschutzrecht nicht anwendbar. Kann der Anwender des Arbeitsassistenzsystems mit vertretbarem Aufwand ermittelt werden oder werden Daten pseudonymisiert verarbeitet, ist Datenschutzrecht zu beachten.

II. Rechtfertigung

Die Verarbeitung von personenbezogenen Daten ist verboten, wenn sie nicht jeweils auf eine Rechtsgrundlage gestützt werden kann. Wichtigste Rechtsgrundlage beim Einsatz adaptiver Arbeitsassistenzsysteme im Beschäftigtenkontext ist die Verarbeitung im

Rahmen des Beschäftigtenverhältnisses nach § 26 BDSG-neu und die Kollektivvereinbarung.

1. Kollektivvereinbarung

Gibt es bereits eine Kollektivvereinbarung, die den Einsatz des geplanten Assistenzsystems abdeckt oder kann eine solche vor Inbetriebnahme geschlossen werden? ☐

Werden in der Kollektivvereinbarung die verarbeiteten Beschäftigtendaten und die Verarbeitungsschritte ausreichend konkretisiert und werden die Interessen der Beschäftigten ausreichend berücksichtigt? ☐

> Eine Kollektivvereinbarung ist eine empfehlenswerte Grundlage für die Verarbeitung von Beschäftigtendaten im Zusammenhang mit adaptiven Arbeitsassistenzsystemen. Die Prozesse können dort genau beschrieben und Maßnahmen zum Schutz der Beschäftigten (Zweckbestimmung, Löschungspflichten) festgelegt werden.

2. Verarbeitung im Rahmen des Beschäftigtenverhältnisses

Gem. § 26 BDSG-neu dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigtenverhältnisses verarbeitet werden, wenn dies für die Durchführung des Beschäftigtenverhältnisses erforderlich ist. In einem ersten Schritt sind die erhobenen Daten und die jeweiligen Verarbeitungszwecke zu ermitteln. Im Rahmen einer Abwägung ist dann zu prüfen, ob die Verarbeitung erforderlich ist.

Zu welchen Zwecken erfolgt die Verarbeitung der Beschäftigtendaten beim Einsatz des adaptiven Assistenzsystems?

Im Regelfall zulässige Zwecke

- Vermittlung von Handlungs- und Prozesswissen
- Kommunikation
- Arbeitsorganisation
- Arbeitserleichterung und Fehlervermeidung
- Effizienzgewinn bei der Prozessgestaltung
- Arbeitsschutz
- Sicherheit des Betriebs

- Kontrolle und Qualitätssicherung
- Ermittlung eines individuellen Qualifizierungsbedarfs ☐

Im Regelfall unzulässige Zwecke:

- Anlasslose Dauerüberwachung
- Erstellung von Beschäftigtenprofilen
- Datensammeln ohne konkreten Zweck oder für später festzulegende Zwecke
- Erstellung von umfassenden Bewegungsprofilen ☐

Welche Daten werden verarbeitet?

Für besonders sensible Daten sind die Hürden für die Zulässigkeit der Verarbeitung höher. Daher muss auch bestimmt werden, welche Daten verarbeitet werden.

Keine besonderen Datenkategorien:

- Name, Anschrift, Beschäftigungsdauer, bisherige Tätigkeiten, Qualifikationen, Alter, Geschlecht
- Prozessdaten über die ausgeübte Tätigkeit
- Standortdaten ☐

Sensible Daten:

- Daten, die Rückschlüsse auf Rasse, ethnische Herkunft, politische, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit erlauben ☐
- Genetische Daten ☐
- Biometrische Daten (Fingerabdrücke, Iris-Erkennung, Stimme, Fotos nur bei eindeutiger Identifizierbarkeit bspw. mittels Gesichtserkennungssystemen) ☐
- Gesundheitsdaten: Alle Daten, die sich auf die körperliche oder geistige Gesundheit des Beschäftigten beziehen, also bspw. Puls, Blutdruck, Blutwerte usw., die von einer Health-App, Fitness-App oder mit Hilfe von Wearables, z.B. Smart Watches, erfasst werden ☐

Ist die Datenverarbeitung zur Erreichung der Zwecke geeignet?

Fördert die Datenverarbeitung den Zweck der Verarbeitung, also bspw. die Vermittlung von Handlungs- und Prozesswissen oder ist die Datenverarbeitung ein ungeeignetes Mittel? ☐

a) Ist die Datenverarbeitung erforderlich?

Besteht die Möglichkeit, den angestrebten Zweck auf andere Weise zu erreichen, bei der der Eingriff in das Recht des Beschäftigten weniger stark ist?

- Können anonymisierte oder pseudonymisierte Daten verwendet werden, ohne dass die Zweckerreichung beeinträchtigt wird? ☐
- Können die Daten unmittelbar nach Zweckerreichung wieder gelöscht werden? ☐
- Kann das angestrebte Ziel auch ohne die Zusammenführung von verschiedenen Daten erreicht werden? ☐

Dem Arbeitgeber steht bei der Wahl des geeigneten Mittels ein weites Maß an unternehmerischem Ermessen zu. So können Arbeitsassistenzsysteme eingeführt werden, auch wenn eine Assistenz auch mit Hilfe von nicht digitalen Mitteln, wie z.B. Handbüchern, möglich ist. Die konkrete Datenverarbeitung muss jedoch auf das tatsächlich erforderliche Maß begrenzt werden.

b) Überwiegen die Interessen des Unternehmens an der Datenverarbeitung gegenüber den Interessen des Beschäftigten?

Wie stark ist der Eingriff in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung des Beschäftigten unter Berücksichtigung der Kategorie der verarbeiteten Daten?

- schwer, weil die Art und Zahl der erhobenen Daten Rückschlüsse bspw. auf Profil, Gesundheit, Arbeitsweise und Standorte des Beschäftigten erlauben oder die Datenverarbeitung eine Dauerüberwachung zur Folge hat ☐

- mittel, weil nach Art und Zahl der verarbeiteten Daten derartige Rückschlüsse nicht möglich sind. Der Beschäftigte hat aber ein Interesse daran, dass derartige Daten nur im notwendigen Umfang verarbeitet werden. ☐

- weniger schwer, weil davon auszugehen ist, dass der Beschäftigte im Regelfall keine Einwände gegen die Verarbeitung dieser Daten hat ☐

Wie wichtig ist die Datenverarbeitung für das Unternehmen unter Berücksichtigung des Eigentumsrechts (Art. 14 GG), der Unternehmensfreiheit (Art. 12 GG) und der Vertragsfreiheit?

- sehr wichtig ☐
- wichtig ☐
- lediglich Ergänzung zu bestehenden Prozessen ☐
- unwichtig ☐

Überwiegen bei einer Gegenüberstellung der Interessen die Interessen des Arbeitgebers unter Berücksichtigung eines unternehmerischen Entscheidungsspielraums bei der Festlegung der Unternehmensprozesse? ☐

Nur wenn man bei Abwägung der jeweiligen Interessen zum Ergebnis kommt, dass die Unternehmensinteressen im konkreten Fall überwiegen, ist die Datenverarbeitung zulässig. Bei überwiegendem Beschäftigteninteresse können Verbesserungen der Beschäftigteninteressen das Abwägungsergebnis verändern, bspw. durch erhöhte Transparenz, frühzeitige Löschung, Pseudonymisierung, Berechtigungskonzepte usw.

Werden Daten für andere als bei der Erhebung vorgesehene Zwecke genutzt?

- Wenn ja, handelt es sich um kompatible Zwecke, d.h. ist der Zweck in der Unternehmensorganisation als ein vergleichbar anzusehender Zweck einzuordnen? ☐

- Insbesondere: Konnte der Beschäftigte mit der Nutzung der Daten für diesen neuen Zweck rechnen? ☐

Grundsätzlich dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden. Die DSGVO erlaubt jedoch eine Zweckänderung, wenn der neue Zweck mit dem alten Zweck kompatibel ist, d.h. insb., wenn der Beschäftigte auch mit einer Datenverarbeitung für diesen Zweck rechnen konnte. Über ein hohes Maß an Transparenz lassen sich Beschäftigtendaten daher auch für andere Zwecke, als bei Erhebung vorgesehen, nutzen.

3. Werden die Daten der Beschäftigten nach Erreichung des jeweiligen Zwecks unter Berücksichtigung etwaiger Aufbewahrungsfristen gelöscht? ☐

Es empfiehlt sich, ein Löschungskonzept zu erarbeiten, in welchem die Daten bestimmten Zwecken und Aufbewahrungsfristen zugeordnet werden, so dass nach Entfallen der Rechtfertigungsgrundlage für die Datenverarbeitung eine unverzügliche Löschung erfolgt.

4. Ist Ihr Unternehmen darauf vorbereitet, den Beschäftigten Auskunft über die jeweils über ihn erhobenen und verarbeiteten Daten zu erteilen? ☐

Nach Art. 15 DSGVO sind Sie auf Wunsch des Betroffenen verpflichtet, Auskunft über die bei Ihnen verarbeiteten Daten zu erteilen und im Rahmen einer allgemeinen Information über Verarbeitungszwecke, Datenkategorien, möglichen Empfängern, Dauer der Speicherung, Herkunft der Daten, automatisierte Einzelentscheidungen, Profiling sowie die bestehenden Rechte aufzuklären. Auszugeben sind ein Informationsblatt und eine Datenübersicht. Die Ausgabe ist durch dokumentierte organisatorische Maßnahmen sicherzustellen.