Besondere Probleme im Beschäftigtendatenschutz und Empfehlungen für ein Beschäftigtendatenschutzgesetz

Zur nationalen Umsetzung der DSGVO

Stand: 18.12.2020

Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel

Karin Schuler
schuler@netzwerk-datenschutz-expertise.de
Kronprinzenstraße 76, 53173 Bonn

www.netzwerk-datenschutzexpertise.de

Inhalt

Das Bundesarbeitsministerium (BMAS) hat einen Beirat eingerichtet, der Empfehlungen für ein neues Beschäftigtendatenschutzgesetz erarbeiten soll. So kann für die 20. Legislaturperiode des Deutschen Bundestags eine valide Grundlage geschaffen werden, um endlich ein Gesetz zum wirksamen Datenschutz von Beschäftigten zu erhalten. Dabei sind die europarechtlichen Vorgaben zu beachten, die dem Beschäftigtendatenschutz auch in Deutschland nachhaltige Impulse geben können. Das vorliegende Gutachten untersucht, welche Problemlagen bei der Überwachung von Beschäftigten und ganz allgemein bei der Verarbeitung von Beschäftigtendaten durch Arbeitgeber bestehen, welche Vorgaben im Europarecht genutzt werden können und wie diese in ein Beschäftigtendatenschutzgesetz einfließen können.

1 Kleine Geschichte des Beschäftigtendatenschutzgesetzes

Die Geschichte des Beschäftigtendatenschutzes in Deutschland war bisher von politischer Unentschiedenheit und richterlicher Kompetenz geprägt: Eigentlich ist schon seit den 70er Jahren des 20. Jahrhunderts klar, dass die Automatisierung und die damit einhergehende Verarbeitung personenbezogener Daten im Betrieb eine Gefahr für das Persönlichkeitsrecht von Beschäftigten darstellt, die durch eine gesetzliche Regulierung gebannt werden sollte.[1] Mit dem **Volkszählungsurteil** des Bundesverfassungsgerichts (BVerfG) wurde eine verfassungsrechtliche Grundlage für den Schutz des gefährdeten Rechts auf informationelle Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts geschaffen.[2]

Dieser Schutz ist nicht nur im Verhältnis zum Staat, sondern auch im Privatrechtsverkehr, also im Wirtschafts- und insbesondere im Arbeitsleben notwendig. Das BVerfG betonte die **staatliche Verantwortung** und die sich aus dem allgemeinen Persönlichkeitsrecht ergebende Pflicht, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten, die es dem Einzelnen möglich und zumutbar macht, sich informationell zu schützen. Diese Schutzpflicht gilt insbesondere für Vertragsverhältnisse, in denen *„ein Partner ein solches Gewicht hat, dass er den Vertragsinhalt faktisch einseitig bestimmen kann“*. In solchen Fällen ist es *„Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt“*. Dies ist insbesondere der Fall, wenn der überlegene Vertragspartner für den anderen *„zur Sicherung seiner persönlichen Lebensverhältnisse von so erheblicher Bedeutung ist, dass die denkbare Alternative, zur Vermeidung einer zu weitgehenden Preisgabe persönlicher Informationen ganz abzusehen, für ihn unzumutbar ist“*.[3] Ein solches Machtungleichgewicht zwischen Vertragspartnern besteht zwischen Arbeitgebern und Beschäftigten und insbesondere im Hinblick auf den Einsatz von Informations- und Kommunikationstechnik (IT) im Unternehmen, der ausschließlich vom Arbeitgeber bestimmt wird.[4]

Angesichts dieser verfassungsrechtlichen Vorgaben war und ist es konsequent, dass der Gesetzgeber normative Vorgaben für einen Interessenausgleich zwischen Arbeitgeber und Beschäftigten macht.[5]

[1] Steinmüller/Lutterbeck/Mallmann/Kolbe/Schneider, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, 1971, BT-Drs. VI/3826, S. 134 f., 155 ff.
[2] BVerfG 15.12.1983 – 1 BvR 209/83 u.a., NJW 1984, 419 ff.
[3] BVerfG 23.10.2006 – 1 BvR 2027/02, Rn. 33-36, JZ 2007, 577.
[4] Schuler/Weichert, S. 12.
[5] Nachweise für die vielfachen Bestrebungen bei Seifert in Simitis, BDSG, 8. Aufl. 2016, § 32 ,Rn. 1.

Seit der Volkszählungsentscheidung des BVerfG vereinbarten die Regierungsparteien immer wieder, ein (damals) **Arbeitnehmerdatenschutzgesetz** zu erlassen. Doch alle Versuche, ein solches Gesetz zu verabschieden, scheiterten letztlich am politischen Widerstand der Arbeitgeberseite.[6] Nur einmal fand sich in einem Koalitionsvertrag keine Selbstverpflichtung zur Verabschiedung eines solchen Gesetzes: in der 2005 beginnenden 16. Legislaturperiode. Just in dieser Periode gab es derart viele Überwachungsskandale im Beschäftigtenbereich in Deutschland, dass sich die CDU-SPD-Regierung 2009 noch kurz vor der nächsten Bundestagswahl genötigt sah, mit dem § 32 Bundesdatenschutzgesetz (BDSG) zumindest minimale Festlegungen ins Gesetz aufzunehmen.[7]

Nicht nur auf nationaler, auch auf **europäischer Ebene** blieben alle Versuche einer Verbesserung des Persönlichkeitsschutzes im Arbeitsverhältnis in ersten Ansätzen stecken.[8] Zwar wurden mit der seit 2009 geltenden europäischen Grundrechte-Charta (GRCh) sowohl ein Grundrecht auf Datenschutz als auch umfassende Arbeitnehmerrechte auf oberster Regulierungsebene garantiert (siehe dazu unter Ziffer 2), doch scheut der europäische Gesetzgeber bisher vor einer präzisierenden Regulierung zurück. Mit der seit 2016 in Kraft befindlichen europäischen Datenschutz-Grundverordnung (DSGVO) traute er sich nur, in Art. 88 einen allgemeinen rechtlichen Rahmen für die nationalen Gesetzgeber sowie für kollektivrechtliche Normen vorzugeben. Die eigentliche Arbeit an einem wirksamen Schutz überließ er den Mitgliedstaaten. Diese können spezifischere Vorschriften vorsehen, die geeignete und besondere Maßnahmen zur Wahrung der Menschenwürde, der berechtigten Interessen und der Grundrechte umfassen, insbesondere im Hinblick auf Transparenz, konzerninterne Kommunikation und Überwachungssysteme am Arbeitsplatz.[9]

Dass der Beschäftigtendatenschutz in Deutschland trotz der politischen Untätigkeit des Gesetzgebers bisher nicht unter die Räder geraten ist, ist insbesondere der **Rechtsprechung**, vor allem des Bundesarbeitsgerichts (BAG), zuzuschreiben. Das BAG nahm in seinen Entscheidungen immer wieder einen angemessenen Ausgleich zwischen den Kontrollinteressen der Arbeitgeber und dem Persönlichkeitsschutz der Beschäftigten vor. Die Gerichte setzten und setzen dem Technikeinsatz Grenzen, etwa bei der Videoüberwachung[10], dem Einsatz biometrischer Verfahren[11], der Auswertung von Tele- und Bürokommunikationsmitteln[12] oder der Verarbeitung von Daten im Internet und sog. sozialen Medien. Dadurch war auch eine Anpassung der Rechtslage an den Einsatz neuer Technologien möglich. Die gerichtliche Kontrolle ist aber immer eine nachträgliche Kontrolle nach Einführung von teilweise mächtigen und teuren Systemen, die sich immer (nur) auf den jeweiligen Einzelfall bezieht. Von den Gerichten nicht veränderbar, weil gesetzlich vorgegeben, sind die prozeduralen Vorgaben, die trotz der technischen Entwicklung nicht angepasst wurden.

Der **Koalitionsvertrag von CDU/CSU und SPD** für die 19. Legislaturperiode ist zur vorliegenden Thematik wenig konkret. Dort beschränkte man sich auf folgende Versprechen:

[6] Schuler/Weichert, S. 7 f.
[7] Gesetz zur Änderung datenschutzrechtlicher Vorschriften v. 14.08.2009, BGBl. I S. 2814.
[8] Schuler/Weichert, S. 3 f. m.w.N.
[9] Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 9 Rn. 6 (S. 134 f.).
[10] BAG 27.03.2003 – 2 AZR 51/02, JZ 2004, 366; BAG 21.06.2012 – 2 AZR 153/11, NJW 2012, 3594; EGMR 09.01.2018 – 1874/13 u. 8567/13, AuR 2019, 32.
[11] LAG Berlin-Brandenburg 04.06.2020 – 10 Sa 2130/19.
[12] BAG 27.07.2017 – 2 AZR 681/16, NJW 2017, 3258 = NZA 2017, 1327.

„Wir unterstützen die Arbeitnehmerinnen und Arbeitnehmer im digitalen Wandel: … Sicherstellung des Beschäftigtendatenschutzes. … Die Einführung digitaler Arbeitsprozesse wie die E-Akte führen zu mehr Transparenz. Dadurch können zum einen Steuerungsinstrumente zur Optimierung entwickelt werden, und zum anderen besteht die Sorge vor dem gläsernen Mitarbeiter. Daher wollen wir Klarheit über Rechte und Pflichten der Arbeitgeberinnen und Arbeitgeber, der Arbeitnehmerinnen und Arbeitnehmer schaffen sowie die Persönlichkeitsrechte der Beschäftigten sicherstellen (Beschäftigtendatenschutz). … Wir wollen die Öffnungsklausel in Artikel 88 der EU-Datenschutz-Grundverordnung nutzen und prüfen die Schaffung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft."[13]

Mit der zugesagten Prüfung wurde mit der Berufung eines „**Beirats zum Beschäftigtendatenschutz**" im Juni 2020 durch das Bundesarbeitsministerium (BMAS) begonnen. Unter der Leitung der früheren Bundesjustizministerin Herta Däubler-Gmelin sollen 14 Mitglieder innerhalb von sechs Monaten Empfehlungen ausarbeiten.[14]

Dabei bezieht sich das BMAS ausdrücklich auf das Gutachten der **Datenethikkommission** (DEK), die u.a. Folgendes ausführt:

„Die DEK empfiehlt der Bundesregierung, die Sozialpartner einzuladen, ausgehend von den bereits in Tarifverträgen bestehenden Beispielen guter Übung eine gemeinsame Linie für gesetzliche Konkretisierungen des Beschäftigtendatenschutzes zu entwickeln. Dabei sollten auch die Belange von Personen in unüblichen Beschäftigungsformen berücksichtigt werden. Kollektivverträge und Betriebsvereinbarungen sollen auch weiterhin im Bereich des Beschäftigtendatenschutzes eine wichtige Rolle spielen. Schon wegen der gesteigerten Grundrechtsrelevanz sollten die zentralen Grundsätze des Beschäftigtendatenschutzes aber nicht ausschließlich an Kollektivverträge und Betriebsvereinbarungen überwiesen werden, zumal diese nicht alle Beschäftigten erfassen. Die gegenwärtig bestehende Rechtsunsicherheit über das Ausmaß, in dem Vorschriften der DSGVO anwendbar bleiben, erschwert überdies sichere Investitionen. … Der Fokus eines Beschäftigtendatenschutzes sollte daher auf spezifisch auf den Beschäftigungskontext zugeschnittene, gesetzliche Rechtfertigungsgründe gelegt werden, die ein hohes Maß an Schutz und einen angemessenen Grundrechtsausgleich gewährleisten. Diese können einwilligungsähnliche Elemente aufweisen, welche die typischerweise gegebenen Machtverhältnisse im Beschäftigungskontext berücksichtigen.

*Bei der Ausgestaltung der Mitbestimmungsrechte der Interessenvertretungen über die Verarbeitung personenbezogener Daten im Betrieb muss der bestehenden **Wissensasymmetrie** zwischen Arbeitgeber- und Arbeitnehmerseite über die Wirkungsweise und Details der Verarbeitungsvorgänge angemessen Rechnung getragen werden. Es müssen daher Modelle gefunden werden, die den Interessenvertretungen über die geltenden Mechanismen hinaus den Rückgriff auf externen Sachverstand ermöglichen, wobei auf eine angemessene Einbindung des betrieblichen Datenschutzbeauftragten, aber auch auf den Schutz von Geschäftsgeheimnissen zu achten ist.*

[13] Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode, 2018, Rn. 361-364, 1833-1838, 6068-6089.
[14] Bundesministerium für Arbeit und Soziales, PM v. 16.06.2020, Beirat zum Beschäftigtendatenschutz nimmt seine Arbeit auf.

Angesichts der ständigen Fortentwicklung datenverarbeitender Systeme im Betrieb (Software-Updates, selbstlernende Elemente usw.) sollte eine Fortentwicklung von punktueller Zustimmung hin zu dauerhafter Begleitung von Prozessen durch die Interessenvertretungen erfolgen. …

Bei einer Weiterentwicklung des Beschäftigtendatenschutzes ist darauf zu achten, dass auch diejenigen Personen erfasst werden, die in unüblichen Beschäftigungsformen arbeiten. Durch die Zunahme unüblicher ***Beschäftigungsformen in der Plattformökonomie*** *verfügen die betreffenden Personen nicht über die klassischen Arbeitnehmer- und Mitspracherechte. Es kann zu einem enormen Machtungleichgewicht zwischen dem Auftraggeber bzw. dem Plattformbetreiber einerseits und dem Auftragnehmer bzw. den über die Plattform Arbeitenden andererseits kommen, das sich auch auf den Datenschutz und die informationelle Selbstbestimmung auswirken kann. Dem ist durch geeignete rechtliche Vorschriften – idealerweise auf EU-Ebene – und die Weiterentwicklung institutioneller Rahmenbedingungen, etwa durch eine Interessenvertretung, entgegenzuwirken."*[15]

2 Rechtliche Vorgaben

Durch die allgemeinen Vorgaben des Art. 88 DSGVO[16] sind, auch wenn dessen Konkretisierung über die darin enthaltene Öffnungsklausel weitgehend den nationalen Normgebern überlassen ist, neben den nationalen verfassungsrechtlichen Vorgaben auch die Regelungen der europäischen Grundrechte-Charta (GRCh) anwendbar. Die GRCh konkretisiert in Art. 8 das vom deutschen Verfassungsgericht über die Rechtsprechung entwickelte Recht auf informationelle Selbstbestimmung, das **Grundrecht auf Datenschutz**, indem die Prinzipien der Zweckbindung, von Treu und Glauben sowie der Auskunftsanspruch und die unabhängige Kontrolle festgeschrieben werden.

Während das Grundgesetz (GG) hinsichtlich des Schutzes von Beschäftigtenrechten sehr zurückhaltend ist, enthält die GRCh weitergehende Regeln: Art. 27 GRCh sichert den Beschäftigten und deren Vertretern *„rechtzeitige* ***Unterrichtung und Anhörung****"* zu. Adressat dieses Anspruchs sind die Arbeitgeber bzw. die beschäftigenden Unternehmen. Gegenstand von Unterrichtung und Anhörung sind alle Aspekte, die für Beschäftigte in ihrer Stellung relevant sind. Hierzu gehören auch die Arbeitsbedingungen und der Einsatz von Informationstechnik im Rahmen der Arbeit.[17] Die Regelung hat eine individualrechtliche wie auch eine kollektivrechtliche Komponente. Dadurch, dass Art. 27 GRCh auf die rechtlichen Vorgaben verweist, wird dem (nationalen) Gesetzgeber zugleich ein Rechtsetzungsauftrag erteilt.[18]

Art. 28 GRCh eröffnet den Beschäftigten wie den Arbeitgebern das Recht, sich kollektiv zu organisieren und kollektiv Regelungen *„auszuhandeln und zu schließen sowie bei Interessenkonflikten* ***kollektive Maßnahmen zur Verteidigung ihrer Interessen****"* zu ergreifen. Dadurch ist sowohl die Selbstorganisation der Beschäftigten in Betriebsräten als auch in Gewerkschaften und die Interessendurchsetzung durch diese abgesichert. Als Maßnahmen der kollektiven Interessenwahrnehmung werden Tarifverträge und Streiks nur beispielhaft aufgeführt. Davon mit erfasst sind auch Betriebsvereinbarungen sowie andere Mitbestimmungsrechte sowie Klagerechte. Die

[15] Gutachten der Datenethikkommission, 2019, S. 112 f.
[16] Zur Geschichte des Art. 88 Schuler/Weichert, S. 4 f.
[17] Holoubek in Schwarze, Art. 27 GRC Rn. 12.
[18] Holoubek in Schwarze, Art. 27 GRC Rn. 18.

Regelung macht keinen Unterschied zwischen der Vertretung von individuellen und kollektiven Interessen.[19]

Art. 31 GRCh begründet für Beschäftigte ein *„Recht auf **gesunde, sichere und würdige Arbeitsbedingungen**“*. Zu den Arbeitsbedingungen gehört der Einsatz von Informations- und Kommunikationstechnik. Deren Einsatz soll daher so gestaltet werden, dass sie möglichst keine Gefahren für die Gesundheit oder für das Persönlichkeitsrecht der Betroffenen erzeugen. Diese Auffassung wird durch den Wortlaut des Art. 31 GRCh bekräftigt, indem der Würdeschutz ausdrücklich erwähnt wird. Letztlich sollen die Arbeitsbedingungen mit sämtlichen den Beschäftigten zustehenden Grundrechten in Einklang stehen.

Art. 88 DSGVO konkretisiert die Sicherung der informationellen Grundrechte von Beschäftigten. Dabei steht zweifellos das Recht auf Schutz personenbezogener Daten nach Art. 8 DSGVO im Vordergrund, schließt aber sämtliche diesem Personenkreis zustehende *„Grundrechte und Grundfreiheiten“* mit ein (vgl. Art. 1 Abs. 2 DSGVO). Die Präzisierung der Vorgaben der DSGVO zur **Datenverarbeitung im Beschäftigtenkontext** obliegt umfassend den Mitgliedstaaten. Dabei legt die DSGVO ein rechtliches Mindestniveau fest, das nicht unterschritten werden darf.[20]

In Art. 88 Abs. 2 DSGVO ist festgelegt, was die normkonkretisierenden Vorschriften, also zum Beispiel ein Beschäftigtendatenschutzgesetz, auf nationaler Ebene umfassen sollen: *„**geeignete und besondere Maßnahmen** zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, 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“.* Dabei handelt es sich um eine exemplarische Nennung von Maßnahmen, ohne sich hierauf zu beschränken. Voraussetzung und Prüfstein für jede Maßnahme und Regelung in einem Beschäftigtendatenschutzgesetz ist, dass sie zur Erreichung dieses Ziels geeignet ist und sich im Rahmen des vorgegebenen europarechtlichen Rahmens bewegt.

Vorschriften i.S.v. Art. 88 DSGVO sind u.a. **§ 26 BDSG sowie § 87 Abs. 1 BetrVG** mit ihren Festlegungen zur Einwilligung, zur Verarbeitung sensitiver Daten, zur Mitbestimmung und zu sonstigen Beteiligungsrechten der Interessenvertretungen der Beschäftigten sowie die Ausweitung des Anwendungsbereichs des Datenschutzes auf die Akten-Datenverarbeitung. Weitere Regelungen finden sich in bereichsspezifischen Gesetzen, so etwa in § 3 Arbeitssicherheitsgesetz (ASiG), §§ 19-22 Gendiagnostikgesetz (GenDG), §§ 106 ff. Bundesbeamtengesetz (BBG) und vielen mehr.[21]

3 Spezifische Probleme des Beschäftigtendatenschutzrechts

Der bei bisherigen Regelungsversuchen zu einem Beschäftigtendatenschutzgesetz verfolgte Ansatz bestand darin, für einzelne **spezifische technische Anwendungen oder Anwendungsklassen** detailliertere Vorgaben zu machen. Diese Vorgaben orientierten sich regelmäßig an der vermuteten Sensitivität der Verarbeitung und formulierten dann sowohl materiell-rechtliche als auch prozedurale

[19] Holoubek in Schwarze, Art. 28 GRC Rn. 11, 19.
[20] Däubler in Däubler u.a., Art. 88 Rn. 14; zum Regelungsansatz der DSGVO generell Schuler/Weichert, S. 6 ff.
[21] Zu den allgemeinen Anforderungen im nationalen Recht ausführlich Schuler/Weichert, S. 13 ff.

Anforderungen. Dieser Ansatz sollte weiterhin verfolgt werden, jedoch sollte nach Wegen gesucht werden, das bestehende Recht angesichts heutiger Herausforderungen anwendbarer zu machen. Denn die Anwendung stößt durch den technologischen Fortschritt oft an Grenzen bei der praktischen Umsetzung. Durch die Multifunktionalität moderner IT-Systeme verschwimmen häufig die Verarbeitungszwecke und damit auch die Rechtsgrundlagen, auf denen die Erhebung der jeweiligen Daten erfolgt.

Personalinformationssysteme beispielsweise werden immer weniger von anderen Systemen hermetisch abgeriegelt. Vielmehr fließen zunehmend Daten auch aus anderen Systemen (z.B. zur Leistungsmessung) in Personalinformationssysteme ein. Dabei überschreiten Datenflüsse häufig nicht nur die Grenzen einzelner Systeme, sondern auch die Grenzen von Unternehmen (z.B. in Konzernzusammenhängen). Insbesondere bei Inanspruchnahme von Cloud-Diensten werden die Personaldaten unterschiedlicher Konzerngesellschaften häufig gar nicht mehr getrennt voneinander verarbeitet – insbesondere nicht getrennt nach evtl. unterschiedlichen Anforderungen der Einzelgesellschaften. Auch der Einsatz von Video- und Audiotechnik, Geotracking, von Mustererkennungsverfahren wie z.B. biometrischer Identifizierung, von Big-Data-Auswertungen oder von modellbasierten, adaptierenden Systemen (vulgo „Künstliche Intelligenz“) erfolgt zunehmend nicht nur zu einem definierten Zweck, sondern oft zu mehreren Zwecken. Systemseitig werden diese Zwecke oft nicht sauber beschrieben, geschweige denn getrennt.[22] Hersteller lassen nicht selten das Verständnis für datenschutzrechtliche Anforderungen vermissen und erschweren durch unzureichende diesbezügliche Dokumentation selbst datenschutzwilligen Kunden die korrekte Analyse, Einsatzdokumentation und letztlich den datenschutzkonformen Einsatz ihrer Software. Auch wenn es sich bei der Multifunktionalität nicht um ein völlig neues Phänomen handelt, so lässt sich doch durch die immer stärkere Vernetzung von Systemen eine Verschärfung der damit einhergehenden datenschutzrechtlichen Probleme beobachten: sowohl nonchalante Zweckänderung als auch unzureichende Systemdokumentation haben zwar immer schon die Datenschutzkonformität beeinträchtigt, aber bei heutigen; komplexen Systemen wirken derartige Versäumnisse geradezu datenschutzverhindernd.

Bei **allen IT-Systemen** schreiten die technische Entwicklung und der Umfang des Einsatzes in den Betrieben weiter voran. Dabei kommt immer mehr Sensorik zur Anwendung, die sich nicht auf Produktionsvorgänge beschränkt und die Beschäftigte in ihrer jeweils aktuellen Situation und Befindlichkeit erfasst. Auch wenn minutiös erfasste Daten ursprünglich einem betriebsablaufbezogenen Zweck dienten, wachsen die Begehrlichkeiten bei Arbeitgebern, sobald die Möglichkeiten der Auswertung für beschäftigtenbezogene Leistungsmessung deutlich werden. Dass hiermit eine Zweckänderung mit allen datenschutzrechtlichen Pflichten verbunden ist, wird nicht selten verdrängt.

Biometrische und biotechnische Verfahren lassen die Grenzen zwischen **Informationstechnik und Biotechnik** verschwimmen. Konkrete Anwendungen können aus Gründen des Arbeitsschutzes oder zwecks einer Optimierung von Arbeitsabläufen sinnvoll oder gar notwendig sein, zugleich aber – bei einer entsprechenden Gestaltung – für die Beschäftigten einen unerträglichen Überwachungsdruck zur Folge haben.

[22] Schuler/Weichert, S. 9 ff.

Es kann daher bei der gesetzlichen Regulierung der Verarbeitung von Beschäftigtendaten nicht ausreichen, mit Hilfe von Ge- und Verboten besondere Anwendungen zu erlauben oder auszuschließen. Vielmehr ist es von Bedeutung, durch eine für alle Beteiligten **transparente Gestaltung eine vertrauenswürdige Datenverarbeitung** im Unternehmen zu verwirklichen, mit der sowohl eine größtmögliche Produktivität wie auch ein größtmöglicher Persönlichkeitsschutz realisiert werden.[23] Letztlich muss es gelingen, Rahmenbedingungen, Leitplanken und auch rote Linien zu definieren, die selbst für heute noch nicht erkennbare Anwendungen ausreichend Orientierung für Verantwortliche und Schutz für Beschäftigte bieten.

Transparente Gestaltung kann oft nur vor Ort bzw. im Betrieb unter Einbeziehung aller **wesentlichen Beteiligten** erreicht werden. Beteiligt sind damit zunächst der Arbeitgeber sowie der Betriebsrat. Schon aus formellen Gründen (Art. 38 Abs. 1 DSGVO) ist zudem weiterhin der (betriebliche) Datenschutzbeauftragte zu beteiligen. Beteiligt werden müssen in vielen Fällen darüber hinaus Plattform-, Cloud- und/oder Software-Anbieter sowie Unternehmen, die die Implementierung eines Verarbeitungssystems im Betrieb verantworten. Insbesondere bei der Weiterentwicklung von Systemen spielen die IT-Administratoren im Betrieb eine wichtige Rolle. Insbesondere wenn kein Betriebsrat gewählt wurde, sind die einzelnen Beschäftigten als Beteiligte relevant.

In diesem Sinne sollen im Folgenden einige Aspekte beleuchtet werden, die in der bisherigen Diskussion um den Beschäftigtendatenschutz nicht im Vordergrund standen, bei einer Neuregelung aber berücksichtigt werden sollten. Lösungsvorschläge zu den in dieser Ziffer 3 beschriebenen Problemfeldern finden sich weiter unten in Ziffer 4.

3.1 Technische Aspekte

3.1.1 Einsatz komplexer Systeme und Verfahren

Es erscheint naheliegend, die Komplexität heutiger Systeme in den Blick zu nehmen, wenn man bestimmte datenschutzrechtliche Problemfelder abgrenzen und Lösungsansätze entwickeln will. Will man allgemeingültige, anwendungsunabhängige Regeln vom Überschreiten einer Komplexitätsgrenze abhängig machen, so muss man Komplexität nachvollziehbar definieren. Denn das intuitive Verständnis, was ein komplexes System ist, ist sowohl subjektiv als auch über die Zeit und durch die Technikentwicklung Änderungen unterworfen. Die Problematik solcher Systeme besteht darin, dass es sich aufgrund der Komplexität um **schwer beherrschbare Systeme** handelt.

Folgende Eigenschaften können solche Systeme charakterisieren:

- die Vernetzung mehrerer, durch verschiedene Zwecke gekennzeichneter Einzelsysteme derart, dass die in einem System erhobenen personenbezogenen Daten zwischen den beteiligten Systemen in beide Richtungen fließen und so den unterschiedlichen Zwecken der Einzelsysteme dienen, obwohl sie nur in einem der beteiligten System erhoben wurden.
- die Nutzung von Hardware und Software, deren Konfiguration nur noch teilweise in der Hand des datenschutzrechtlich Verantwortlichen liegt und von diesem nur noch bedingt beeinflusst werden kann, wie dies z.B. bei Cloud-Lösungen und „as a Service“-Lösungen der Fall ist (vgl. Ziffer 3.1.2).

[23] Zur Gefahr einer Verrechtlichungsfalle und den prozeduralen Alternativen auch Schuler/Weichert, S. 17 f.

- der Einsatz von Software zur Emotionsanalyse, Gesichtserkennung oder zur automatisierten Analyse und Bestimmung von Identität, Befindlichkeit oder zur Vorhersage wahrscheinlichen Verhaltens von Personen, wobei biometrische oder gar biotechnische Sachverhalte erfasst und weiterverarbeitet werden,[24]
- die Nutzung modellbasierter, adaptierender Technologien zur Verarbeitung personenbezogener Daten, deren Verarbeitungsergebnisse nicht mehr ausreichend durch Menschen kontrolliert werden und mit denen automatisiert unkontrollierte Diskriminierungen erfolgen können.

3.1.2 Plattformen und As-A-Service-Modelle

Eine praktische Erfahrung, u.a. bei der Verhandlung von Betriebsvereinbarungen ist, dass Unternehmen Hard- und Software zum Einsatz bringen oder bringen wollen, deren Funktionsweise von ihnen selbst nicht (völlig) verstanden, geschweige denn durchdrungen wurde. Dazu trägt unter anderem bei, dass heutige Cloud-Systeme („as a Service"-Modelle) oft nur noch sehr rudimentär über fachgerechte System- und Softwaredokumentation verfügen. Viele **Hard- und Software-Angebote** kommen zudem von global agierenden Unternehmen, die ihre Angebote nicht an den Anforderungen der jeweiligen nationalen Rechtsordnungen orientieren, in denen sie zum Einsatz kommen sollen. Dies trifft in jedem Fall auch zu, wenn ein Unternehmen Social-Media-Angebote etwa von Facebook, Google oder Amazon nutzt, bei denen auch Beschäftigtendaten mitverarbeitet werden.

Betriebsräte und Datenschutzbeauftragte werden immer häufiger damit konfrontiert, dass **Systeme von der Stange** eingesetzt werden sollen, die nicht verständlich dokumentiert sind und angeblich von den externen Anbietern oder im konkreten Einsatz nicht mehr (datenschutzgerecht) angepasst werden können. Sind hingegen Anpassungen in bestimmtem Rahmen möglich (Customizing), sind diese selten kostenfrei erhältlich. Betriebsräten und Datenschutzbeauftragten wird so mindestens die „Schuld" an angeblich unangemessen teuren Anpassungen gegeben, wenn sie diese im Sinne des Beschäftigtendatenschutzes fordern.

3.2 Organisatorische Aspekte

3.2.1 Tracking und Zweckänderung

Einige Wirtschaftsbranchen sind dadurch gekennzeichnet, dass sich zur Erbringung ihrer Dienstleistung stark digitalisierte Abläufe etabliert haben, bei denen große Mengen an Daten gesammelt werden. Diese Daten sind dann notwendig, um die Dienstleistung in der zugesicherten Form zu erbringen. Dies betrifft beispielsweise Lieferdienste, Logistikanbieter und Online-Händler. Die Trackingdaten, die das Unternehmen für die Leistungserbringung erheben muss, sind jedoch gleichzeitig beschäftigtenbezogen. Wenn ein Auslieferungsfahrzeug jederzeit zu orten ist, um dem Kunden die Zustellzeit nennen zu können, können auch Leistung und Verhalten von Fahrern und Fahrerinnen des Unternehmens ausgewertet werden. Die minutiöse Verfolgung von Waren auf Ihrem Weg in das und aus dem Regal eines Online-Händlers enthält oft ebenso einen Bezug zu den jeweiligen Beschäftigten (Wer hat die Ware wann eingeräumt? Wer hat die Ware wann aus dem Regal geholt? Wer hat das Paket an den Kunden gepackt?). Ist der Personenbezug beim einzelnen Datensatz möglicherweise zunächst lediglich „unabdingbare Beigabe", werden die entstandenen Massendaten nicht selten für einen ganz anderen Zweck genutzt, z.B. zur minutiösen Leistungsfeststellung und zum engmaschigen

[24] Zur Sprachanalyse bei Stellenbewerbern Betz, ZD 2019, 148.

Leistungsvergleich. Die eigentlich für Zwecke der Leistungserbringung erhobenen Daten werden so zur Quelle für Hitlisten (Wer hat letzten Monat die meisten Kunden angefahren?) und „Berechnung“ von Leistungsvorgaben („Sie haben seit zwei Wochen nur 60% der durchschnittlichen Leistung Ihrer Kolleg.innen erzielt.“). Dass diese Nutzung von Daten datenschutzrechtlich eine Zweckänderung bedeutet, geht meist bei der Datennutzung unter; der Arbeitgeber darf schließlich grundsätzlich die Leistungserbringung durch die Beschäftigten überwachen. Wie weit diese Zweitnutzung im Einzelfall tatsächlich gehen darf und ab wann von einer unzumutbaren, lückenlosen und unerlaubten Dauerüberwachung auszugehen ist, ist oft unklar und juristisch umstritten, aber dringend klärungsbedürftig.

Häufig ähnlich unerwartet für die betroffenen Beschäftigten entstehen neue Möglichkeiten der Leistungs- und Verhaltenskontrolle durch die Koppelung von weitgehend ohne Personenbezug arbeitenden Steuerungssystemen mit (Produktions-) Planungssystemen, in denen personenbezogene Daten verarbeitet werden.

3.2.2 Individuelle Rechte der Beschäftigten

Das Grundrecht auf Datenschutz hat vorrangig eine individualrechtliche Dimension. Unabhängig vom abgeleiteten kollektivrechtlichen Schutz durch Mitbestimmung gewährt das Datenschutzrecht jedoch auch Beschäftigten alle **Rechte von Betroffenen**. Dazu gehören insbesondere die Rechte auf Information (Art. 13 DSGVO) und Auskunft (Art. 15 DSGVO).

Während in vielen Branchen mit umfangreicher Datenerhebung und -verarbeitung (z.B. in der. Versicherungsbranche) den betroffenen Versicherten inzwischen sehr detailliert gefasste **Informationsblätter** bereitgestellt werden, ist dies im Unternehmensbereich gegenüber den betroffenen Beschäftigten häufig nicht der Fall. Dabei besteht das Problem nicht vorrangig darin, dass überhaupt keine Information bereitgestellt würde (das wäre bereits jetzt ein Rechtsverstoß), sondern dass die Informationen häufig völlig oberflächlich und unzusammenhängend gestaltet werden.

Oft beschränken sich derartige Informationen auch auf die klassischen Personalverwaltungsdaten; der Umgang mit Beschäftigtendaten, die durch die **dienstlich veranlasste Nutzung von Systemen** entstehen (Logdateien, Produktivitätsauswertungen, Schichtpläne, Zeiterfassung, Videoüberwachung usw.) wird ohne nachvollziehbare Beschreibung erwähnt oder gleich schlichtweg „vergessen“. Auch finden sich selten konkrete, begründete Löschfristen, sondern meist der Hinweis auf „gesetzliche Aufbewahrungsfristen, die einzuhalten“ seien. Da es für viele anfallende Beschäftigtendaten schlichtweg keine gesetzlichen Aufbewahrungsfristen gibt (Logdateien, einzelne Kommt/Geht-Datensätze, Mails usw.) dient die formelhafte Angabe meist nur als Ausrede für eine nicht vorhandene Angabe und als Vertuschung nicht vorhandener Löschkonzepte.

Auch wird der Versuch, gegenüber dem Arbeitgeber das **Auskunftsrecht** wahrzunehmen, von diesem meist als lästig, wenn nicht gar als Unbotmäßigkeit empfunden. Aus nicht ganz nachvollziehbaren Gründen scheinen viele Arbeitgeber der Ansicht zu sein, dass die besondere Enge des Arbeitsverhältnisses einen qualifizierten Auskunftsanspruch des Beschäftigten entbehrlich macht. Wird dann, widerwillig, nach mehreren Aufforderungen und nach Ausschöpfung aller Argumente bzgl. unzumutbaren Umfangs schließlich nachgegeben, ist das Ergebnis oft dürftig. Nicht gerade selten macht man sich keine Mühe, in Bezug auf Datenkategorien, Verarbeitungen (insbesondere

Auswertungen) und Löschfristen Vollständigkeit und für den Betroffenen die nötige Aussagekraft zu erzielen.

Welcher Detaillierungsgrad erforderlich ist, um dem gesetzlich intendierten Ziel der Übersichtsgewinnung und des **Verständnisses des Betroffenen** zu genügen, ist weder für aktive noch für passive Auskünfte eindeutig bestimmt, so dass eine Auseinandersetzung mit dem Arbeitgeber häufig zu einer langwierigen und nicht selten erfolglosen Angelegenheit wird.

3.2.3 Rollenvermischung Beschäftigter - Privatperson

Es ist eine uralte Praxis, dass Arbeitgeber ihre Beschäftigten auch dadurch an sich zu binden versuchen, dass sie diesen Sonderkonditionen für den Kauf oder die Nutzung der **Produkte des Unternehmens** anbieten. Hiergegen ist nichts einzuwenden. Aus Datenschutzsicht problematisch wird es jedoch, wenn diese Praxis Datenspuren in der beschäftigungsrelevanten Datenverarbeitung des Arbeitgebers hinterlässt und so der Arbeitgeber Informationen über seine Beschäftigten erhält, die ihm nicht zustehen. Das Konsumverhalten der Beschäftigten sollte für deren Bewertung im Anstellungsverhältnis keine Auswirkungen haben. Ein im Gesundheitswesen tätiger Arbeitgeber sollte Gesundheitsdaten seiner Beschäftigten nicht über das unbedingt nötige Maß hinaus erfahren. Eine Bank sollte die finanziellen Verhältnisse ihrer Beschäftigten nicht im Beschäftigungskontext nutzen. Eine solche Datenverwendung steht im Widerspruch zum datenschutzrechtlichen Zweckbindungsrundsatz (Art. 5 Abs. 1 lit. b DSGVO). Die Nutzung von Informationen aus dem privaten Bereich für arbeitsrechtliche Zwecke beeinträchtigt schutzwürdige Betroffeneninteressen. Die private Sphäre darf keine Auswirkungen auf das Beschäftigungsverhältnis haben. Daten, die der Arbeitgeber als Dienstleister von Beschäftigten erhält, dürfen nicht in Zusammenhang mit Beschäftigtendaten gebracht werden.

Weniger eindeutig ist die Trennbarkeit zwischen Privatem und Dienstlichem beim Einsatz privater Geräte als Arbeitsmittel. Das weit verbreitete Phänomen, das unter dem Kürzel BYOD (**Bring your own Device**) beschrieben wird, führt dazu, dass betriebliche Daten auf privaten Geräten Beschäftigter verarbeitet werden, auf die der Arbeitgeber keine Zugriffsrechte hat. Versucht er, um seiner Verantwortung für die Datenverarbeitung wenigstens ansatzweise gerecht zu werden, im Rahmen seiner Direktionsbefugnisse gegenüber dem Beschäftigten die Nutzung des Privatgeräts zu kontrollieren, verletzt er das Eigentums- und Persönlichkeitsrecht betroffener Beschäftigter. Ein Einblick in die private Nutzung des Geräts, das vom Beschäftigten umfangreich und in vielen Lebenslagen verwendet wird (Smartphone, Privat-PC, PKW), ist ein unzulässiger Übergriff des Arbeitgebers in die Privatsphäre des Beschäftigten und muss ausgeschlossen werden. Hierfür gibt es inzwischen einfache technische Lösungen zur Trennung zweier Sphären auf einem Gerät. Diese finden aber in der Praxis sehr oft keine Anwendung, weil sie der administrativen Planung und Betreuung bedürfen.

Aus datenschutzrechtlicher Sicht besonders heikel ist es, wenn der Beschäftigte nicht nur einzelne Geräte, sondern seine Wohnung dienstlich nutzt. Die Praxis der Arbeit im **Home-Office** hat im Rahmen der Corona-Pandemie eine große Bedeutung erlangt. Dabei erfolgen sowohl eine zeitliche als auch eine räumliche Vermengung von Privatem und Dienstlichem. Die Kontrolle des Beschäftigten durch den Arbeitgeber macht es unabdingbar, dass zumindest begrenzt in die besonders geschützten Privatbereiche der Wohnung, der Kommunikation und des Familienlebens eingegriffen wird. Dabei stellen sich Probleme bei der Dokumentation der Arbeitszeit, dem Umgang mit sensiblen Unterlagen

bis hin zur Sicherstellung der Arbeitsergebnisse. Diese lassen sich nur begrenzt durch technische Hilfen lösen und bedürfen einer zusätzlicher normativen Flankierung.[25] Verantwortungsvolle Arbeitgeber schließen mit ihren zuhause arbeitenden Beschäftigten Zusatzverträge zum Arbeitsvertrag, in denen verbindliche Regeln, Verhaltensweisen und Arbeitsanweisungen vereinbart werden. Ein auch in solchen Vereinbarungen kaum aufzulösender Konflikt besteht zwischen dem Grundrecht auf Unverletzlichkeit der Wohnung einerseits und einem zur Sicherstellung vereinbarter Schutzregeln erforderlichen Betretungsrecht des Arbeitgebers, bzw. dessen Vertretern (Revisoren, Datenschutzbeauftragte) andererseits.

3.2.4 Gefährdung von Whistleblowern

Whistleblowing erfüllt eine wichtige Funktion in einem rechtstaatlichen demokratischen Arbeitsleben. Die Praktiken von Unternehmen entsprechen nicht in jedem Fall den rechtlichen und ethischen Standards. Beschäftigte, die von rechtswidrigen oder **unethischen Praktiken** Kenntnis haben, müssen eine verlässliche und sichere Möglichkeit erhalten, um diese außerhalb der betroffenen Organisation zur Kenntnis zu bringen. Umgekehrt müssen Unternehmen vor **unberechtigten anonymen Anschuldigungen** geschützt werden.

Das deutsche Arbeitsrecht gewährleistet bisher keinen angemessenen Schutz von Whistleblowern, denen der Verlust ihres Arbeitsplatzes und weitere Nachteile bis hin zur existenziellen Gefährdung drohen.[26] Daran hat auch das Gesetz zum Schutz von Geschäftsgeheimnissen[27] nichts Grundsätzliches geändert, das vor Schadensersatzforderungen und Unterlassungsforderungen des Arbeitgebers schützen kann, nicht aber vor **arbeitsrechtlichen Folgen**.[28] Die EU hat nun eine Whistleblower-Richtlinie[29] erlassen, die einen umfassenderen Schutz anstrebt, indem Unternehmen mit 50 und mehr Beschäftigten verpflichtet werden, ein internes Whistleblowing-System für die Meldung von Verstößen gegen das EU-Recht einzurichten. Die Richtlinie, die einen über sie hinausgehenden Regelungsspielraum belässt, ist bis zum 17.12.2021 in nationales Recht umzusetzen und wurde bisher noch nicht nationalstaatlich umgesetzt.

3.2.5 Rechtsstellung von Dienstleistern

Die Verlegung und Nutzung von immer mehr Systemen und Beschäftigtendaten zu Dienstleistern und offenen Plattformen erfordert datenschutzrechtlich eine vertragliche Absicherung durch den Arbeitgeber. Während bei einfachen Dienstleistungen (Software as a Service und vergleichbare) innerhalb der EU inzwischen die Anbieter selbst vorbereitete Verträge zur **Auftragsverarbeitung** mit den gemäß Art. 28 Abs. 1, 3, 4, 9 DSGVO erforderlichen detaillierten Regelungen anbieten, ist die Sachlage bei außereuropäischen Anbietern und öffentlichen Plattformen komplizierter.

[25] Problemaufriss bei Verheyen/Elgert K&R 2020, 476.
[26] EGMR 21.07.2011 – 2827/08 (Heinisch/Deutschland), NJW 2011, 3501.
[27] § 5 Nr. 2 GeschGehG v. 18.04.2019, BGBl. I S. 466 in Umsetzung der EU-Richtlinie 2016/943 v. 08.06.2016, ABl. 2016 L 157/1; generell dazu Ulrici, Geschäftsgeheimnisschutzgesetz, 2019.
[28] Böning zit. in Reinsch, SZ 05./06.09.2020, 59; vgl. Apel/Walling, DB 2019, 897; Aszmons/Herse, DB 2019, 1849; Dann/Markgraf, NJW 2019, 1777; Fuhlrott/Hiéramente, DB 2019, 969.
[29] Richtlinie (EU) 2019/1937 v. 23.10.2019, ABl. L 305/17; Weidmann, DB 2019, 2393.

Werden beispielsweise Social-Media-Angebote eingesetzt, liegt regelmäßig eine **gemeinsame Verantwortung** des Arbeitgebers mit dem oder den externen Anbietern vor.[30] Diese setzt gemäß Art. 26 Abs. 1 S. 2 DSGVO eine Vereinbarung voraus, in der u.a. in transparenter Form festgelegt sein muss, welcher der Verantwortlichen *„welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt“*. So soll diese Vereinbarung die Angabe einer Anlaufstelle für die Betroffenen (Art. 26 Abs. 1 S. 3 DSGVO) enthalten; bei der Verarbeitung von Beschäftigtendaten sollte dies der Arbeitgeber sein.

Sowohl bei einer gemeinsamen Verantwortlichkeit als auch bei einer Auftragsverarbeitung stellen sich zudem weitere **Dokumentationspflichten**, die sich insbesondere aus den Art. 5 Abs. 2 (Rechenschaftspflicht, Rechtmäßigkeitsnachweis), 30 (Verarbeitungsverzeichnis) und 35 (Datenschutz-Folgenabschätzung - DFA) DSGVO ergeben. Der Betriebsrat hat nach § 80 Abs. 2 BetrVG insofern ein umfassendes Einsichtsrecht (vgl. Ziffer 3.3).

Nach solchen Verträgen, insbesondere zur gemeinsamen Verantwortung, fragen Betriebsräte ihre Arbeitgeber oft vergeblich. Während die Bedingungen und Notwendigkeiten einer Auftragsverarbeitung sich im Laufe der Jahre herumgesprochen haben, können viele Arbeitgeber mit den Charakteristika und den Erfordernissen einer gemeinsamen Verantwortung wenig anfangen. Betriebsräte werden nicht selten mit der Klage abgespeist, man könne doch wohl nicht erwarten, dass die „Global Player“ der Software-Entwicklung mit einem kleinen deutschen Unternehmen einen maßgeschneiderten Vertrag über die von der Datenverarbeitung betroffenen Prozesse schließen.

3.2.6 Drittstaatentransfer

Ein großes Problem, vor allem für Konzernunternehmen, besteht, wenn Teile der Beschäftigtendatenverarbeitung nicht beim deutschen Arbeitgeber erfolgt, sondern in einem außerhalb des EU/EWR-Raums befindlichen Drittstaat, bei dem von der EU-Kommission **keine Angemessenheit des Datenschutzniveaus** gemäß Art. 45 DSGVO anerkannt worden ist. Dies betrifft u.a. in den USA ansässige Konzernmütter, die sich zunächst auf den Safe-Harbor-Beschluss von 2000 und dann auf den Privacy-Shield-Beschluss von 2015 berufen haben. Nach den Unwirksamkeitserklärungen von Safe Harbor[31] und Privacy Shield[32] durch den Europäischen Gerichtshof (EuGH) sind die Grundlagen für die Datentransfers in die USA mit sofortiger Wirkung weggefallen. Mit dem letztgenannten Urteil war nämlich durch den EuGH zudem klargestellt worden, dass ein Datentransfer von der EU in ein Drittland zwar grundsätzlich über die von der EU-Kommission genehmigten Standarddatenschutzklauseln gerechtfertigt werden könne, dass aber jeweils zusätzlich geprüft werden muss, ob den vom europäischen Recht gestellten Anforderungen tatsächlich genügt wird. Dies ist nur der Fall, wenn für die Betroffenen durchsetzbare Rechte und wirksame Rechtsbehelfe

[30] EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = JZ 2018, 1154 = NZA 2018, 919 = MMR 2018, 591 = BB 2018, 1480 = ZD 2018, 1386 = DuD 2018, 518; EuGH 10.07.2018 – C-25/17 (Zeugen Johovas), NJW 2018, 285 = NZA 2018, 991 = NVwZ 2018, 1787; EuGH 29.07.2019 – C-10/17 (Social-Plug-In/Fashion ID), NJW 2019, 2755 = DuD 2019, 723 = CR 2019, 574 = NZA 2019, 1125 = MMR 2019, 579 = BB 2019, 1995 = K&R 2019, 562.
[31] EuGH 06.10.2015 – C-362/14 (Schrems I), NJW 2015, 3151 = NVwZ 2016, 43 = WM 2015, 2383 = MMR 2015, 753 = K&R 2015, 710 = DÖV 2015, 1070 = JZ 2016, 360 = DuD 2015, 823.
[32] EuGH 16.07.2020 – C-311/18 (Schrems II), NJW 2020, 2613 = WM 2020, 1495 = DB 2020, 1612 = K&R 2020, 588 = DuD 2020, 685.

gewährleistet werden. Dies gilt insbesondere auch, wenn auf die transferierten Daten beim Datenimporteur durch staatliche Behörden zugegriffen wird bzw. werden kann.[33]

In seiner Entscheidung zum Privacy Shield wird vom EuGH klargestellt, dass angesichts der Massenüberwachung durch US-Geheimdienste und dem fehlenden Rechtsschutz für die Betroffenen ein Datentransfer in die USA problematisch ist, ohne dass dieser völlig ausgeschlossen sein müsste. Schon in den bestehenden Standarddatenschutzklauseln ist vorgesehen, dass ein Datenimporteur den Exporteur zu unterrichten hat, falls er seine vertraglich geregelten Datenschutzpflichten nicht einhalten kann, was zur Folge haben muss, dass die übermittelten Daten zurückgeschickt oder zerstört werden müssen.[34] Ergänzend ist festzuhalten, dass die Datenverarbeitung einer unabhängigen Aufsicht unterliegen muss und Rechtsschutz zu gewährleisten ist. Dies lässt sich dadurch realisieren, dass vertraglich der Datenimporteur zu einer umfassenden Auskunft gegenüber dem Exporteur und dessen Datenschutzaufsicht verpflichtet wird und den Betroffenen beim Exporteur in Europa bzw. in Deutschland auch bzgl. der Datenverarbeitung in den USA umfassender Rechtsschutz zugesprochen wird. Einen Vorschlag für einen solchen Export-Import-Vertrag machte das Netzwerk Datenschutzexpertise schon Anfang des Jahres 2016.[35] Entsprechende Sicherungen sind nicht nur beim Datenaustausch mit den USA nötig, sondern bei jedem Empfängerland, bei dem keine **unabhängige Datenschutzaufsicht und kein umfassender Rechtsschutz** gewährleistet sind.

Die beschriebene Problematik betrifft Beschäftigtendaten in ganz besonderer Weise. Klassische Personaldaten enthalten regelmäßig besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO (Gewerkschaftszugehörigkeit, Schwerbehinderung, Schwangerschaft, BEM-Maßnahme, körperliche Einschränkungen, die bestimmte Möbel erfordern usw.) und müssen daher ganz besonders vor unberechtigter Einsichtnahme geschützt werden. Bei der Bestimmung angemessener Garantien und Schutzmaßnahmen bei einer außereuropäischen Verarbeitung ist zu bedenken, dass das Risiko eines unberechtigten Zugriffs auf Beschäftigtendaten wegen des Umfangs des betrieblichen Profils regelmäßig sehr hoch ist.

3.2.7 Rechtsfolgen von Verstößen

Anders als das Strafprozessrecht (vgl. §§ 69 Abs. 3, 136a, 252 StPO) kennt das Zivilrecht kein **Beweisverwertungsverbot**. Vielmehr erfolgt die Beantwortung der Frage, ob unzulässig erhobene Beweismittel prozessual verwendet werden dürfen, im Rahmen einer freien richterlichen Beweiswürdigung (§ 46 Abs. 2 ArbGG, § 286 Abs. 1 S. 1 ZPO). Dies ist angesichts des Machtungleichgewichts zwischen Arbeitgeber und Beschäftigten zu hinterfragen: Der Arbeitgeber kann sich veranlasst sehen, Datenschutzvorschriften, wozu auch durch Betriebsvereinbarung geregelte Auswertungsbeschränkungen gehören, zu ignorieren., Die Aussicht, dass auch unrechtmäßig erlangte Beschäftigtendaten vor Gericht als Beweismittel zugelassen werden können und seine Rechtsverstöße letztlich zu seinen Gunsten wirken, fördert nicht eben die Rechtstreue des Arbeitgebers. (z.B. in Kündigungsverfahren).

Das BAG leitet zwar ein Beweisverwertungsverbot grundsätzlich aus der Verfassung ab, ist aber in seiner Judikatur nicht einfach einzuschätzen. Zuletzt hat es ausdrücklich eine Entscheidung darüber

[33] EuGH 16.07.2020 – C 311/18 Rn. 105, 194-197.
[34] EuGH 16.07.2020 – C 311/18 Rn. 139-143.
[35] https://www.netzwerk-datenschutzexpertise.de/dokument/anforderungen-export-import-vertrag; ebenso Schuler/Weichert DuD 2016, 386.

abgelehnt, *„ob die Betriebsparteien gegenüber den Gerichten über das formelle Recht hinausgehende Verwertungsverbote begründen“* können.[36] Datenschutzverstöße, die mit einem erheblichen materiellen Eingriff in das allgemeine Persönlichkeitsrecht einhergehen, können ein Beweisverwertungsverbot begründen. Kleinere und formelle Verstöße sowie Verstöße gegen die Mitbestimmungspflicht nach dem BetrVG werden tendenziell nicht als Grund für ein Verwertungsverbot anerkannt.[37] Im Ergebnis besteht angesichts der **offenen Abwägung** und sehr unterschiedlichen Bewertungen in der juristischen Literatur hohe Rechtsunsicherheit. Die in Betriebsvereinbarungen häufig verwandten Klausel, wonach dem Arbeitgeber untersagt wird, unrechtmäßig (also entgegen den Bestimmungen einer Betriebsvereinbarung) erlangte Daten und Erkenntnisse in ein Gerichtsverfahren einzubringen, ist demnach wenig belastbar.

Gesetzlich und auch gerichtlich nicht geklärt ist auch, inwieweit **Verstöße gegen das Mitbestimmungsrecht**, soweit es dem Persönlichkeitsschutz der Beschäftigten dient, als Datenschutzverstoß zu bewerten sind, die von Datenschutzaufsichtsbehörden im Rahmen ihrer Tätigkeit ermittelt und sanktioniert werden können.

3.3 Mitbestimmungsaspekte

3.3.1 Information des Betriebsrates

Gemäß § 80 Abs. 1 BetrVG hat der Betriebsrat darüber zu wachen, dass die **zugunsten der Arbeitnehmer geltenden Regelungen** durchgeführt werden. Gemäß § 80 Abs. 2 hat er demnach in allen Fällen, Abläufen und Vorhaben die von Schutzvorschriften des Abs. 1 betroffen sind, zunächst ein Recht auf rechtzeitige und umfassende Information. Dieses Recht besteht vollkommen unabhängig von der Frage, ob der in Rede stehende Sachverhalt möglicherweise weitere Beteiligungsrechte des Betriebsrats auslöst (wie z.B. Mitbestimmung). Dem Betriebsrat sind die erforderlichen Unterlagen zur Verfügung zu stellen, die er zur Wahrnehmung seiner Beteiligungsrechte benötigt. In Bezug auf den Datenschutz hat die Regelung zur Folge, dass der Betriebsrat einen Anspruch darauf hat, die in den Art. 26 (Vereinbarung gemeinsamer Verantwortlicher), 28 (Verträge über Auftragsverarbeitung), 30 (Verzeichnis von Verarbeitungstätigkeiten), 35 (Datenschutz-Folgenabschätzung) DSGVO genannten Dokumente zu erhalten, soweit es dabei (auch) um die Verarbeitung von Beschäftigtendaten geht. Auch benötigt er zur Wahrnehmung seiner Mitbestimmung bei IT-Systemen nach § 87 Abs. 1 Nr. 8 BetrVG Unterlagen, die gleichermaßen als Teil der Systembeschreibung gelten und datenschutzrechtliche Pflichten darstellen. Dazu gehören: die vollständige Aufzählung betroffener Beschäftigtendaten, die Entwicklung und Dokumentation eines Berechtigungskonzepts und die Erstellung und Dokumentation eines Löschkonzepts. Tatsächlich erhalten Betriebsräte diese Dokumente aber zumeist nicht rechtzeitig, d.h. umgehend nach der Erstellung, sondern erst auf Anforderung, manchmal nur lückenhaft – und manchmal überhaupt nicht. Es ist leider noch immer keine Selbstverständlichkeit, dass die rechtlich geforderten und fachlich unabdingbaren Dokumente erstellt werden, so dass sie auch dem Betriebsrat bereitgestellt werden könnten. Wem auch immer im Einzelfall Versäumnisse anzulasten sind – Software-Herstellern oder den nutzenden Unternehmen - hat dies zur Folge, dass der Betriebsrat im Hinblick auf IT-Systeme seinen Aufgaben nicht oder zumindest nicht rechtzeitig nachgehen kann.

[36] BAG 31.1.2019 – 2 AZR 426/18
[37] Z.B. BAG 27.07.2017 – 2 AZR 681/16; Überblick bei Akkilic, NZA 2020, 626 f.; Däubler, Gläserne Belegschaften, Rn. 388a ff.

3.3.2 Mitbestimmung des Betriebsrates

Es ist weitgehend unbestritten, dass der Betriebsrat bei der Einführung von informationstechnischen Systemen, die Beschäftigtendaten verarbeiten, gemäß § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht hat. Die Regelung über die „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ wird vom Bundesarbeitsgericht (BAG) dahingehend ausgelegt, dass schon die **Überwachungseignung** die Mitbestimmungspflicht auslöst.[38] Diese Interpretation ist aber angesichts der offenen Formulierung auslegungsbedürftig.[39] Gemäß dem BetrVG bestehen bei einer eine Reihe weiterer Sachverhalte Beteiligungsrechte, so etwa bei Arbeitszeitregelungen (§ 87 Abs. 1 Nr. 2)[40] oder beim Einsatz von Personalfragebögen (§ 94 Abs. 1). Zwar sind die Mitbestimmungsregelungen im BetrVG technikneutral; sie sind aber angesichts der technischen Entwicklung und den damit verbundenen Risiken für das Persönlichkeitsrecht der Beschäftigten nicht mehr hinreichend, da die verwendeten IT-Systeme einem dauernden Wandel (Updates, Releases, zusätzliche Verknüpfungen) unterworfen sind, die von der Regelung nicht hinreichend abgedeckt sind.

Unternehmen wollen moderne IT-Systeme meist zentral einsetzen. Dies führt dazu, dass immer seltener örtliche Betriebsräte die Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG faktisch wahrnehmen können. Wenn ein System über Betriebs- oder sogar Unternehmensgrenzen hinweg eingesetzt werden soll, jedoch auf einer einheitlichen Plattform betrieben wird, können bestimmte Konfigurationen nur einmal für alle festgelegt werden. Es ist nicht möglich, dass beispielsweise der Betriebsrat eines betroffenen Werkes eine Löschfrist für Protokolldateien von zwei Wochen vereinbart, der Betriebsrat eines zweiten Werks, in dem das gleiche System genutzt wird, jedoch eine Löschfrist von 4 Wochen. Ist ein GBR errichtet, führt dieser potenzielle Konflikt auf örtlicher Ebene unmittelbar zu dessen originärer Zuständigkeit, so dass zumindest durch den GBR die Mitbestimmung wahrgenommen werden kann.

3.3.3 Datenschutzdefizite bei fehlender Mitbestimmung

Das individualrechtliche Grundrecht auf Datenschutz wird durch kollektivrechtliche Instrumente ergänzt und bietet so zusätzlich wirksame Garantien im Beschäftigungsverhältnis. Diese Instrumente sind aber im Bereich von Beschäftigungsverhältnissen dann nicht verfügbar, wenn es im Betrieb **keinen Betriebsrat** gibt.

Vergleichbar sind Fälle, in denen zwar örtliche Betriebsräte errichtet sind, diese die Mitbestimmung aber wegen fehlender Zuständigkeit nicht wahrnehmen können. Derartige Konstellationen ergeben sich, wenn kein Konzernbetriebsrat errichtet wurde (wozu es, anders als bei einem GBR, auch bei Vorliegen der Voraussetzungen keine Verpflichtung gibt), der Konzern des Arbeitgebers aber auf Konzernebene ein IT-System einführen möchte. Da eine örtliche Regelung wegen des technischen Zwangs zur Einheitlichkeit nicht getroffen werden kann, verlagert sich die originäre Zuständigkeit zum KBR. Gibt es diesen jedoch gar nicht, so kann die Mitbestimmung völlig verweigert werden.[41] Dies führt dazu, dass gerade komplexe Systeme, wenn sie auf Konzernebene eingeführt werden sollen, in der

[38] BAG 06.12.1983 – 1 ABR 43/81, NJW 1984, 1476 = VersR 1984, 560 = BB 1984, 850 = DB 1984, 775 = JR 1985, 264; BAG 11.03.1986 – 1 ABR 12/84, NJW 1986, 2724 = VersR 1986, 1199 = BB 1986, 1292, 665 = DB 1986, 1469.
[39] So verneinte z.B. das VG Berlin 14.11.2019 – 61 K 8.19 PVL das Mitbestimmungsrecht bei einer Migration von Windows 10 zu Office 2016, DB 2020, 1743.
[40] Weichert in Hans-Böckler-Stiftung (Hrsg.), Arbeitszeiterfassung und mobile Beschäftigung, 2019, S. 175 ff.
[41] So jedenfalls BAG 14.12.1993 – 3 AZR 618/93 Rn. 46, NZA 1994, 556; dazu Salaman NZA 2019, 283 ff.

beschriebenen Konstellation an den örtlichen Betriebsräten vorbei ohne jegliche Mitbestimmung eingeführt werden können.

In allen diesen Fällen sind die einzelnen Arbeitnehmer ihrem Arbeitgeber, was die Entscheidung über den IT-Einsatz sowie den Umfang und die Nutzung erhobener Beschäftigtendaten angeht, weitgehend machtlos ausgeliefert: Der Arbeitgeber verfügt über die Entscheidungskompetenz zum IT-Einsatz und insofern über personelle, finanzielle, informationelle und rechtliche Ressourcen, denen der vereinzelte Arbeitnehmer bisher nur wenig entgegensetzen kann. Zwar stehen ihm die Betroffenenrechte (vgl. Ziffer 3.2.2) und evtl. Schadenersatzansprüche, Art. 82 DSGVO zu. Doch bedarf es auch zu deren Durchsetzung hinreichender Ressourcen und vor allem einer Lage, sich den Konflikt mit dem Arbeitgeber auch leisten zu können. Angesichts der schlechten Ausstattung der Datenschutzaufsichtsbehörden stellt deren Anrufung (Art. 77 DSGVO) in der Regel keinen geeigneten Ersatz für betriebsrätliche Unterstützung dar. Insofern ist diese Option nicht geeignet, das **Machtungleichgewicht** ausrechend zu kompensieren.

3.3.4 Hinzuziehung von Sachverständigen

Der Betriebsrat kann gemäß § 80 Abs. 3 BetrVG *„nach näherer Vereinbarung mit dem Arbeitgeber Sachverständige hinzuziehen, soweit dies zur ordnungsgemäßen Erfüllung seiner Aufgaben erforderlich ist“*. Im Betriebsrat besteht regelmäßig weder die rechtliche noch die technische Kompetenz, um IT-Planungen des Arbeitgebers aus datenschutzrechtlicher Sicht hinreichend zu beurteilen. Daher ist er auf die Hinzuziehung externen Sachverstands angewiesen. Die einbezogenen Sachverständigen müssen das Vertrauen des Betriebsrats genießen und die Fähigkeit haben, die auftretenden Fragestellungen dem Betriebsrat zu vermitteln.

Häufig nutzen Arbeitgeber die nicht ausreichend klare Formulierung des BetrVG dazu, dem Betriebsrat externen Sachverstand unter Hinweis auf interne „sachkundige Auskunftspersonen“ zu verweigern. So sollen beispielsweise Beschäftigte der IT-Abteilung dem Betriebsrat Auskunft geben. Diese Herangehensweise verkennt jedoch, dass es sich bei Beschäftigten der IT-Abteilung weder um unabhängige Sachverständige handelt, noch dass diese oft den speziellen Bezug von Beschäftigteninteressen zum jeweiligen IT-System erkennen. Das ist der Regelfall: IT-Beschäftigte empfinden jede intensivere Nachfrage als Angriff auf ihre Tätigkeit, mauern in Bezug auf vollständige Informationsgewährung und lassen das Verständnis für Aufgaben, Wünsche und Sichtweisen der Beschäftigtenvertretung vermissen.

Versucht der Betriebsrat dennoch, externen Sachverstand zu erhalten, blockiert der Arbeitgeber dies nicht selten durch langwierige Stundensatzdiskussionen, Begrenzung auf einen sachlich ungerechtfertigten Beratungsumfang oder schlichtes Verschleppen.

3.3.5 Beziehung Betriebsrat - Datenschutzbeauftragter

Bisher haben die Regelungen zum Betriebsrat im BetrVG und zum Datenschutzbeauftragten (Art. 37-39 DSGVO, § 38 BDSG) keinen Bezug zueinander. Obwohl es die Aufgabe beider Einrichtungen ist, das **Persönlichkeitsrecht der Beschäftigten zu wahren,** findet eine Zusammenarbeit zu selten statt. Oftmals verschanzt sich der oder die betriebliche Datenschutzbeauftragte gar hinter der Aussage „für den Beschäftigtendatenschutz“ sei „der Betriebsrat zuständig“ und klammert diesen Bereich aus der eigenen Tätigkeit aus.

4 Lösungsvorschläge

Von Arbeitgeberseite wird bei der Diskussion über ein Beschäftigtendatenschutzgesetz regelmäßig vorgetragen, dass **das Arbeitsrecht und das Datenschutzrecht** nicht miteinander vermischt werden sollten bzw. gar dürften. Diese Argumentation blendet aus, dass die beiden Bereiche nicht zu trennen sind: Die DSGVO nimmt ausdrücklich auf das Arbeitsrecht Bezug (in Art. 9 Abs. 2 lit. b, h, Art. 88 Abs. 1). Umgekehrt wird das Arbeitsrecht mit der Digitalisierung der Arbeit immer datenschutzlastiger. Auch kann das Mitbestimmungsrecht in Bezug auf den Einsatz von IT-Systemen regelmäßig nur durch die Vereinbarung von Maßnahmen zum Schutz des Persönlichkeitsrechts von Beschäftigten wirksam umgesetzt werden.

Aufgabe einer gesetzlichen Regelung des Beschäftigtendatenschutzes muss es daher sein, die bisher in unterschiedlichen Gesetzen geregelten Bereiche und **Vorgaben zusammenzuführen und zu harmonisieren**. Dies gilt neben dem Datenschutz insbesondere für das kollektive Arbeitsrecht, allen voran das BetrVG. Welcher Regelungsort vom Gesetzgeber letztlich gewählt wird, sollte sich an der Praktikabilität und Verständlichkeit orientieren. Es erscheint sinnvoll, im Rahmen der Novellierung des Beschäftigtendatenschutzes neben einem spezifischen eigenen Gesetz (im Rahmen eines Artikelgesetzes) auch das BetrVG und evtl. das Tarifvertragsgesetz (TVG) zu ergänzen.

Hinsichtlich des **materiell-rechtlichen Regelungsbedarfs** in einem Beschäftigtendatenschutzgesetz gibt es schon eine Vielzahl von Vorschlägen und Diskussionen. Angesichts der insofern weitgehend akzeptierten Rechtsprechung, die dadurch normiert werden würde, dürfte insofern weitgehend Einigkeit hergestellt werden können.[42]

4.1 Beherrschbarkeit der Technik

4.1.1 Folgenabschätzung

Eine rechtliche Reaktion im Datenschutzrecht auf die besonderen Risiken technischer Verfahren besteht darin, dass vom Verantwortlichen eine **Datenschutz-Folgenabschätzung** (Art. 35 DSGVO) abverlangt wird. Diese ist insbesondere erforderlich bei einer systematischen und umfassenden Erfassung und Auswertung von Daten und einer umfangreichen Verarbeitung sog. sensitiver Daten (Art. 9 Abs. 1 DSGVO) und auch bei einer komplexen und arbeitsteiligen Datenverarbeitung (s.o. 3.1). Der Verantwortliche, im Bereich von Beschäftigungsverhältnissen also der Arbeitgeber, ist verpflichtet, im Rahmen der Folgenabschätzung den Nachweis zu erbringen, dass der Datenschutz über *„zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt“* wird (Art. 35 Abs. 7 lit. d DSGVO).

Bei der Ausarbeitung der Folgenabschätzung ist der Rat des Datenschutzbeauftragten einzuholen (Art. 35 Abs. 2 DSGVO). Einzuholen ist außerdem der „Standpunkt der betroffenen Personen oder ihrer Vertreter“ (Art. 35 Abs. 9 DSGVO). Vertretung auf betrieblicher Ebene ist der Betriebsrat. Der Betriebsrat ist also vor endgültiger Festlegung der Folgenabschätzung mit den „Abhilfemaßnahmen“ zu konsultieren. Diese schon mit der DSGVO gegebene Rechtslage bedarf der nationalrechtlichen Spezifizierung. In einem Beschäftigtendatenschutzgesetz ist daher eine Regelung zu empfehlen,

[42] Schuler/Weichert, S. 22.

wonach schon bei der Durchführung einer Datenschutz-Folgenabschätzung der **Rat des Betriebsrats einzuholen** ist.

Den Aufsichtsbehörden sollte in Anlehnung an Art. 35 Abs. 4 DSGVO aufgegeben werden, in der zu erstellenden **Liste** explizit einen eigenen Abschnitt zu Anwendungen mit Beschäftigtendaten zu erstellen und zu veröffentlichen. Dabei sollte auch festgelegt werden, dass komplexe System im Sinne der Beschreibung in Ziffer 3.1.1 in jedem Fall einer DFA bedürfen.

4.1.2 Zertifizierung

Mit einer unabhängigen transparenten Datenschutzzertifizierung kann das Informationsungleichgewicht zwischen einem IT-Anbieter und den IT-Anwendern durch Zwischenschaltung einer **vertrauenswürdigen und kompetenten Instanz** zumindest teilweise nivelliert werden. Dadurch kann auch das Informations- und Bewertungsdefizit, das oft beim Arbeitgeber gegenüber den von ihm eingeschalteten Plattform- und Serviceanbietern reduziert werden. Die Verteilung von Aufgaben und Verantwortlichkeiten bei einer gemeinsamen Verantwortung oder einer Auftragsverarbeitung werden dadurch offengelegt. Dies gilt in verstärktem Maße für das Informations- und Bewertungsdefizit, das bei der Arbeitnehmervertretung besteht. Dabei soll eine Zertifizierung in Bezug auf den Beschäftigtendatenschutz zweierlei bewirken: sie soll eine auf sachgerechter Systemdokumentation beruhende Aussage zur Möglichkeit eines datenschutzkonformen Betriebs treffen (und so unzureichend dokumentierte Systeme von vorneherein ausschließen) und sie soll Beschäftigtenvertretungen die Arbeit erleichtern. Ein Ersatz für die Mitbestimmung kann damit nicht verbunden sein.

Art. 42 DSGVO macht detaillierte Vorgaben für eine kontrollierte Datenschutzzertifizierung. Es ist damit zu rechnen, dass spätestens im Jahr 2021 die ersten erfolgreichen Zertifizierungen vorgenommen werden. Schwerpunkt der Zertifizierungsüberlegungen sind bisher Cloud-Angebote.[43] Es bietet sich aber an, einen ähnlichen Schwerpunkt im Bereich der Verarbeitung von Beschäftigtendaten zu setzen. Art. 42 Abs. 3 DSGVO sieht vor, dass die Zertifizierungen freiwillig und transparent sind. Die Freiwilligkeit zielt darauf ab, das Eigeninteresse des Verantwortlichen an der Nutzung dieses Bewertungsangebots zu stärken. Sie schließt aber nicht aus, dass der Betriebsrat und der Arbeitgeber als Verantwortlicher sich – z.B. in einer Betriebsvereinbarung – darauf verpflichten, bei bestimmten IT-Anwendungen eine Zertifizierung durchzuführen.[44] Ebenso wenig ausgeschlossen ist, dass gesetzliche Anreize geschaffen werden, Zertifizierungen zwischen Betriebsrat und Arbeitgeber zu vereinbaren. Damit wird vielmehr der in Art. 42 Abs. 1 DSGVO geregelten staatlichen Förderpflicht hinsichtlich der Zertifizierung entsprochen.[45]

Demgemäß sollte in einem Beschäftigtendatenschutzgesetz ausdrücklich geregelt werden, dass der **Nachweis der Möglichkeit, bei entsprechender Konfiguration Datenschutzkonformität** in einem im Arbeitsverhältnis zum Einsatz kommenden IT-Systemen zu erzielen, durch eine Zertifizierung nach Art. 42 DSGVO erbracht werden kann.

[43] Zum aktuellen Stand siehe die Beiträge in DuD 10/2020 von Krasemann und Gühr/Karper/Maseberg.
[44] Weitergehend Weichert in Däubler u.a., Art. 42 Rn. 9, 29.
[45] 42 Rn. 20.

4.2 Organisatorische Vorgaben und Ansätze

4.2.1 Vorbedingungen für Zweckänderungen

Es muss klargestellt werden, dass nicht alle im Arbeitsprozess anfallenden Daten ohne Einschränkung für jegliche Leistungskontrolle von Beschäftigten verwendet werden dürfen. Der Umstand, dass der Arbeitgeber die Erfüllung der arbeitsvertraglich geschuldeten Leistung überprüfen darf, rechtfertigt keine schrankenlose Verwendung von für betriebliche Prozesse erhobenen Daten für die kleinteilige Leistungsmessung von Beschäftigten. Dieser Grundgedanke findet seine normative Umsetzung in Art. 6 Abs. 4 lit. c, d DSGVO, wonach die Sensitivität von Daten und die Folgenschwere einer Zweckänderung für den Betroffenen Kriterien dafür sind, eine Unvereinbarkeit von Verarbeitungszwecken anzunehmen.

Art. 6 Abs. 4 lit. e DSGVO stellt klar, dass die Zulässigkeit einer Zweckänderung vom „Vorhandensein geeigneter Garantien“ abhängig gemacht werden kann. Eine solche Garantie kann darin bestehen, dass gesetzlich eine spezifische Mitbestimmungspflicht festgelegt wird. Für den Fall, dass im Betriebsprozess anfallende Daten für die Leistungskontrolle verwendet werden sollen, sollte gesetzlich klargestellt werden, dass in einer Betriebsvereinbarung Schutzvorkehrungen vorzusehen sind. Eine solche Zweckänderung ist gesetzlich zu untersagen, wenn der durch die zweckfremde Datenverarbeitung ausgelöste Kontrolldruck für die Beschäftigten nicht zumutbar ist.

4.2.2 Prozessstandschaft

Die in Art. 80 Abs. 1 DSGVO eröffnete Möglichkeit, dass gemeinwohlorientierte Interessensvertretungen in Prozessstandschaft für Betroffene umfassend Datenschutzrechte geltend machen können, ist im deutschen Recht bisher nicht umgesetzt worden.[46] Eine Umsetzung im Beschäftigungskontext drängt sich aber angesichts des Machtungleichgewichts, das zwischen Beschäftigten und Arbeitgeber besteht, geradezu auf. Dies gilt insbesondere für Unternehmen, in denen kein Betriebsrat besteht und bei denen deshalb bisher keine **kollektive Rechtswahrnehmung** möglich ist (s.o. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Hierdurch kann ein Betätigungsfeld für Gewerkschaften eröffnet werden.

4.2.3 Trennung Beschäftigter – Privatperson

Die informationelle Trennung zwischen Dienstlichem und Privatem des Beschäftigten sollte zunächst dadurch normativ gewährleistet werden, dass klargestellt wird, dass Informationen aus der Kundenbeziehung zum Unternehmen des Arbeitgebers nicht für Zwecke des Beschäftigungsverhältnisses genutzt werden dürfen.

Bezüglich der Verwendung privater Geräte als Arbeitsmittel sollte ein normatives Gebot zur Nutzung **technischer Trennungsmöglichkeiten** erfolgen, verbunden mit dem Verbot für den Arbeitgeber, auf den privaten Teil der Datenverarbeitung zuzugreifen.

Arbeitgeber sollten verpflichtet werden, für dienstliche Erfordernisse nötige technische Geräte zur Verfügung zu stellen, statt auf die Nutzung privater Geräte (mit allen damit verbundenen datenschutzrechtlichen und haftungsrechtlichen Problemen) zu vertrauen.

[46] Weichert in Däubler u.a., Art. 80 Rn. 10.

Bezüglich der Zutrittsrechte des Arbeitgebers zur Wohnung von Beschäftigten, die im Home-Office arbeiten, sollten klare Rahmenbedingungen und Begrenzungen formuliert werden, die dem Arbeitgeber die notwendigen Kontrollpflichten ermöglichen, jedoch gleichzeitig den Eingriff in die Privatsphäre von Beschäftigten minimieren (z.B. Pflicht zu vorheriger, rechtzeitiger Anmeldung, Beschränkung auf relevante Räume, Beschränkung auf bestimmte Personen).

Die konkrete Ausgestaltung aller Regelungen mit Bezug auf die betrieblichen Gegebenheiten hat ihren richtigen Standort in Betriebsvereinbarungen in Verbindung mit arbeitsvertraglichen Ergänzungen.

4.2.4 Whistleblowerregelung

In Umsetzung der Whistleblower-Richtlinie sollte der deutsche Gesetzgeber eine umfassende Regelung vornehmen, bei welcher der Persönlichkeitsschutz durch prozedurale und technische Vorgaben sowie durch einen materiellen **Schutz vor Offenlegung der Identität** des Whistleblowers und zugleich der Schutz des Arbeitgebers vor unberechtigten anonymen Beschuldigungen gewährleistet wird (s.o. 3.2.4).[47] Hierzu hat das Bundesjustizministerium einen Referentenentwurf mit gesetzlichen Vorschlägen erarbeitet.[48] Eine derart ohnehin wegen EU-Rechtsvorgaben notwendige Regulierung könnte im Rahmen eines umfassenden Gesetzes zum Beschäftigtendatenschutz getroffen werden.

4.2.5 Drittstaatentransfer

Die eindeutige Rechtsprechung des EuGH zum Datentransfer in Drittstaaten ohne ein angemessenes Datenschutzniveau legt es nahe, die höchstgerichtlichen Vorgaben im Bereich des Beschäftigtendatenschutzes **nationalstaatlich normativ zu präzisieren** (s.o. 3.2.6). Art. 88 DSGVO mit seiner Öffnungsklausel gibt diesen Weg frei.

Dies kann in der Weise erfolgen, dass klargestellt wird, dass Datenimporteure als die Empfänger von Beschäftigtendaten gegenüber dem Arbeitgeber als Datenexporteur sowie gegenüber dessen Aufsichtsbehörde umfassend informationspflichtig sind, dass die Aufsichtsbehörde des Arbeitgebers bzgl. der Verarbeitung beim Importeur eine Kontrollkompetenz hat, die vertraglich zwischen Exporteur und Importeur abgesichert werden muss, und dass den Betroffenen gegenüber dem Arbeitgeber auch in Bezug auf die Verarbeitung beim Importeur umfassender Rechtsschutz zugestanden wird. In welcher **rechtlichen Form** die nötigen Garantien abgesichert werden, ist muss nicht gesetzlich vorgegeben werden. Dies kann im Rahmen von erweiterten Standarddatenschutzklauseln erfolgen, über verbindliche interne Datenschutzvorschriften in Konzernen (Binding Corporate Rules, Art. 47 DSGVO) oder durch einen separaten Export-Import-Vertrag zwischen Datenexporteur und Datenimporteur.

4.2.6 Rechtsfolgen von Rechtsverstößen

Die Einheitlichkeit unserer Rechtsordnung verbietet es, bei Verstößen gegen das Persönlichkeitsrecht im Rahmen personenbezogener Datenverarbeitung zwischen Arbeitsrecht und Datenschutz streng zu unterscheiden. Bei derartigen Verstößen besteht (auch) eine Zuständigkeit der Datenschutzaufsichtsbehörden, auch wenn sich der Verstoß in der **Verletzung des BetrVG** oder sonstiger arbeitsrechtlicher Regelungen liegt. Wegen der insofern bestehenden Rechtsunsicherheit sollte dies in einem Beschäftigtendatenschutzgesetz ausdrücklich klargestellt werden, ohne dass

[47] Rottenwallner, VR 2020, 189 ff, 217 ff.
[48] Roßmann, Lambrecht will Whistleblower schützen, www.sueddeutsche.de/politik/whistleblower-schutz-lambrecht-1.5145688, 12.12.2020.

bestehende arbeitsrechtliche oder betriebsverfassungsrechtliche Konfliktlösungs- und Sanktionsmöglichkeiten (gerichtliche Klärung, Arbeit von Einigungsstellen etc.) beschnitten werden.

Bisher besteht kein gesetzliches **Beweisverwertungsverbot** bei Datenschutzverstößen des Arbeitgebers in Beschäftigungsverhältnissen. Angesichts der bestehenden Rechtsunsicherheit empfiehlt es sich, eine gesetzliche Regelung aufzunehmen, in der Kriterien benannt werden, wann ein Verwertungsverbot besteht und wann nicht. Daraus sollte auch hervorgehen, welche Anforderungen die Bestimmung eines Beweisverwertungsverbots in einer Betriebsvereinbarung erfüllen muss.

4.2.7 Einrichtung eines Kompetenzzentrums Beschäftigtendatenschutz

Die Entwicklung von Verhaltensregeln, das Entwerfen von Konzepten, die Eingang in Tarifverträge finden können, die praxisorientierte Datenschutz- Bewertung von IT-Systemklassen und das Festlegen von Kriterien für die datenschutzrechtliche Zertifizierung bewegen sich in einem **Interessendreieck zwischen Arbeitgeber, Arbeitnehmer und Datenschutzaufsicht**.[49]

Zugleich sind diese Aufgaben stark technikgesteuert und juristisch-regulativ hoch anspruchsvoll. Insofern ist es geboten, eine Institution zu schaffen, welche die bestehenden Interessen zusammenführen und zu einem Ausgleich bringen kann, die zugleich mit **hoher Fachkompetenz und hoher Autorität** ausgestattet ist. Ihre Arbeit soll gleichermaßen praxisgerechte und rechtskonforme Empfehlungen ermöglichen, die eine empfehlende Wirkung entfalten ohne rechtssetzende Wirkung zu entfalten (vergleichbar den Hinweisen des Europäischen Datenschutzausschusses gemäß Art. 70 Abs. 1 lt. f-m DSGVO).

Hierfür bietet es sich an, beim **Bundesarbeitsministerium** ein Kompetenzzentrum für den Beschäftigtendatenschutz einzurichten, dem die o.g. Aufgaben zugewiesen werden. Dieses sollte mit hinreichenden personellen und technischen Ressourcen ausgestattet werden. Dessen unabhängiges Entscheidungsgremium sollte zu gleichen Teilen von praxiserfahrenen Vertretern der Arbeitgeber, der Arbeitnehmer und der Datenschutzaufsicht besetzt werden.

4.3 Gestaltung der Mitbestimmung

4.3.1 Mitbestimmungsrecht

Die bisherige Regelung des § 87 Abs. 1 Nr. 6 BetrVG gibt dem Betriebsrat ein weitgehendes Mitbestimmungsrecht beim Einsatz von IT-Systemen, das de facto den Bereich des Datenschutzes umfasst. Angesichts der beschriebenen technischen (Fort-)Entwicklung, der Anforderungen an praktikable Vereinbarungen sich schnell ändernder Systeme und weil technische, organisatorische und prozedurale Maßnahmen immer untrennbarer die betriebliche Nutzung bestimmen, ergibt sich die Gefährdung für Beschäftigte nicht mehr aus den Systemen allein. Der Schutzgedanke des BetrVG, Beschäftigte vor den zur Leistungs- und Verhaltenskontrolle geeigneten Systemen schützen zu wollen, greift daher heute zu kurz. Vielmehr kann sich aus der Gesamtheit aus Systemen, eingebetteten Abläufen, Maßnahmen und Dienstleistern eine hohe Relevanz für die Beschäftigten entwickeln. Daher sollte die Mitbestimmungspflicht derart verändert werden, dass zusätzlich zum IT-System selbst alle verbundenen Maßnahmen mit **Auswirkungen auf das Persönlichkeitsrecht** der Mitbestimmung zugeführt werden.

[49] Vgl. Schuler/Weichert, S. 23 mit dem Vorschlag eines „Datenschutzbeirats“.

Abgrenzungsprobleme werden dadurch nicht vollständig beseitigt. Doch würde über eine solche umfassendere Mitbestimmungspflicht das Schutzziel näher bestimmt und an die Regelung der DSGVO angepasst. Denn der Regelungsansatz der DSGVO beschränkt sich nicht auf das Grundrecht auf Datenschutz, sondern hat ein umfassendes Verständnis des Persönlichkeitsrechts, das generell „**Grundrechte und Grundfreiheiten** natürlicher Personen“ bei der Verarbeitung personenbezogener Daten einschließt (Art. 1 Abs. 2 DSGVO).[50]

4.3.2 Verhältnis Betriebsrat-Datenschutzbeauftragter

Aus den unter Ziffer 3.3.5 **Fehler! Verweisquelle konnte nicht gefunden werden.**,dargelegten Gründen erscheint es sinnvoll, die Tätigkeit von Betriebsrat und Datenschutzbeauftragtem zu verschränken, ohne dass die jeweilige Unabhängigkeit und spezifische Funktion in Frage gestellt wird. Um dies zu erreichen, sollte dem Betriebsrat ein **Vorschlags- und Mitbestimmungsrecht** bei der Benennung des Datenschutzbeauftragten zugestanden werden.[51] Zugleich sollte klargestellt werden, dass angesichts der Überschneidung von Aufgaben ein gegenseitiges Informations- und Unterstützungsrecht besteht. Dadurch würde eine Rechtssituation geschaffen, die den Datenschutzbeauftragten nicht eindeutig im Lager der Unternehmensleitung verortet. Dies schafft auch die Voraussetzung dafür, eine interne Datenschutzkontrolle des Betriebsrats und seiner personenbezogenen Datenverarbeitung sicherzustellen.[52] Zugleich würde dadurch auch die unergiebige Diskussion beendet, ob es sich bei der Beschäftigtenvertretung um einen eigenständigen datenschutzrechtlich Verantwortlichen i.S.v. Art. 4 Nr. 7, 24 ff. DSGVO handelt.[53] Um die Unabhängigkeit des Betriebsrats zu wahren, ist gesetzlich klarzustellen, dass zwischen Betriebsrat und Datenschutzbeauftragtem bezüglich möglicher Kontrollen und Kontrollergebnisse Vertraulichkeit gewahrt wird; insbesondere im Verhältnis zum Arbeitgeber. Die Schweigepflicht des Datenschutzbeauftragten gemäß Art. 38 Abs. 5 DSGVO sollte insofern ausdrücklich zugunsten der Beschäftigtenvertretung gelten.

4.3.3 Hinzuziehung von Sachverständigen

Die Regelung des § 80 Abs. 2 BetrVG ist im Hinblick auf die Einführung und den Betrieb von IT-Systemen zu offen. Eine starke Verbesserung kann schon dadurch erreicht werden, dass die einzusetzenden Verfahren zuvor einer erfolgreichen Zertifizierung unterzogen worden sind (dazu 4.1.2). Diese Zertifizierung wird aber in vielen konkreten Fällen nicht vorliegen; der konkrete Einsatz der Technik im Betrieb bedarf in jedem Fall einer **fachkundigen Kontrolle und Begleitung**.

Daher sollte ein **gesetzlich geregeltes Verfahren** etabliert werden, das sicherstellt, dass der Betriebsrat sich frühzeitig fachkundigen und vertrauenswürdigen externen Sachverstand zur Seite holen kann. Insbesondere im Falle komplexer IT-Systeme im Sinne der Charakterisierung in Ziffer 3.1.1 sowie bei der Inanspruchnahme von Plattformen (s.o. 3.1.2) sollte der Arbeitgeber dem Betriebsrat die Wahrnehmung externer Unterstützung nicht durch Verweis auf interne Auskunftspersonen verweigern können. Ein solches Verfahren kann in die Erarbeitung einer Datenschutz-Folgenabschätzung integriert

[50] Weichert in Däubler u.a., Art. 1 Rn. 19 ff.
[51] Zur bisherigen Rechtslage Däubler, Gläserne Belegschaften, Rn. 599b.
[52] Zur bisherigen Rechtslage BAG 11.11.1997 – 1 ABR 21/97, NJW 1998, 2466 = DB 1998, 627 = NZA 1998, 385 = BB 1998, 106, 648, 897 = JR 1998, 484.
[53] Dazu Weichert in Däubler u.a., Art. 4 Rn. 89a m.w.N.

werden. Es muss jedoch gewährleistet bleiben, dass hierbei die praktischen Bedürfnisse des Betriebsrates beachtet werden und dass die Kostentragung durch den Arbeitgeber gesichert bleibt.

4.3.4 Verhaltensregeln und überbetriebliche Kollektivvereinbarungen

Als Instrument zur Konkretisierung der Anforderungen an spezifische Systeme und Verarbeitungen sieht die DSGVO in Art. 40 **Verhaltensregeln** vor, die auch Vorgaben für Datenschutz-Folgenabschätzungen machen können (Art. 35 Abs. 8 DSGVO). Zumindest insofern ist auch der Standpunkt der Vertretung der Betroffenen einzuholen (vgl. Art. 35 Abs. 9 DSGVO).[54] Innerbetrieblich ist dies der Betriebsrat oder der Personalrat. Auf überbetrieblicher Ebene erfolgt die Vertretung durch Gewerkschaften. Zwar sieht die DSGVO bzgl. der Ausarbeitung von Verhaltensregeln keine Pflicht zur Einbeziehung von Betroffenenvertretungen vor. Sie schließt aber nicht aus, dass eine solche Pflicht nationalgesetzlich geregelt wird, soweit – wie im Bereich des Beschäftigtendatenschutzes gemäß Art. 88 DSGVO – eine Öffnungsklausel besteht. Es empfiehlt sich daher, in einer gesetzlichen Regelung die Ausarbeitung von Verhaltensregeln im Beschäftigtenbereich davon abhängig zu machen, dass der Rat der zuständigen Arbeitnehmervertretungen einzuholen ist.

Um eine höhere Verbindlichkeit i.S.v. Art. 88 DSGVO zu erreichen, sind auf überbetrieblicher Ebene **Tarifverträge** zu Datenschutzfragen zugelassen.[55] Erzielt also ein Branchenverband mit Gewerkschaften Einvernehmen bzgl. spezifischer Regeln zur Datenverarbeitung zu Beschäftigten in einer bestimmten Branche, so können diese gemäß Art. 88 DSGVO für die Beteiligten Verbindlichkeit erlangen.

Art. 40 DSGVO schließt nicht aus, dass Tarifvertragsregelungen zum inhaltlichen Gegenstand von Verhaltensregeln genommen werden. Voraussetzung für die Verbindlichkeit von Verhaltensregeln gegenüber den Aufsichtsbehörden ist aber, dass diese von der zuständigen **Aufsichtsbehörde genehmigt** werden (Art. 40 Abs. 5 DSGVO). Eine Genehmigung von Tarifverträgen durch die Aufsichtsbehörden wäre aber ein Eingriff in die Tarifhoheit der Tarifparteien. Kein solcher Eingriff, sondern eine sinnvolle Verschränkung von Arbeitsrecht und Datenschutzrecht wäre es aber, wenn die Tarifparteien bei Tarifvertragsregelungen angehalten werden, den Rat oder die Stellungnahme der Aufsichtsbehörde einzuholen.

4.3.5 Verbandsklage

Art. 80 Abs. 2 DSGVO ermöglicht es den EU-Mitgliedstaaten, dass sie Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht im Bereich des Datenschutzes Klagerechte einräumen. Dazu müssen die Organisationen satzungsmäßig Ziele im öffentlichen Interesse verfolgen und im Bereich des Datenschutzes tätig sein. Sie dürfen dann unabhängig von einem Auftrag durch Betroffene tätig werden und Beschwerden einlegen und die in den Art. 78, 79 DSGVO aufgeführten Rechte in Anspruch zu nehmen, „*wenn ihres Erachtens die Rechte einer betroffenen Person gemäß dieser Verordnung infolge einer Verarbeitung verletzt sind*“. Von diesem Recht hat Deutschland im Jahr 2016 durch eine Änderung des Unterlassungsklagegesetzes (UKlaG) Gebrauch gemacht, indem es in § 2 Abs. 2 eine Nr. 11 einführte, wonach Verbraucherschutzverbände bei der Verletzung von

[54] ErwGr 99 DSGVO, Weichert in Däubler u.a. Art. 40 Rn. 15.
[55] Schuler/Weichert, S. 20.

Datenschutzgesetzen einen **Unterlassungs- oder einen Beseitigungsanspruch** haben, den sie auch gerichtlich durchsetzen können.[56]

Eine entsprechende Regelung zu einem kollektiven Rechtsschutz ist auch im Hinblick auf den **Beschäftigtendatenschutz** nach Art. 88 DSGVO für Beschäftigtenvertretungen möglich. Es steht dem nationalen Gesetzgeber frei, den Gewerkschaften und Betriebsräten die Möglichkeit einer Rechtewahrnehmung nach Art. 80 DSGVO zu eröffnen.[57] Dies gilt auch für Betriebsräte, denen nur eine beschränkte Rechtsfähigkeit zusteht. Die Rechtsfähigkeit kann entsprechend erweitert werden. Eine solche Rechtsänderung ist geboten, da damit Individualklagen vermieden und eine schnelle und zugleich kompetent vertretene gerichtliche Klärung streitiger Datenschutzfragen im Beschäftigungskontext erreicht werden kann.

5 Abschlussbemerkungen

Angesichts der bisherigen Erfahrungen mit dem Widerstand der Arbeitgeberseite gegen die Kodifizierung des Beschäftigtendatenschutzes dürfte es unrealistisch sein, dass vom Bundestag in der 19. Legislaturperiode noch ein Gesetz hierzu verabschiedet werden wird. Dessen ungeachtet sind die Bestrebungen des BMAS, über einen Beirat die Grundzüge eines Beschäftigtendatenschutzgesetzes zu erarbeiten, unbedingt zu unterstützen. Sie können die Grundlage dafür schaffen, dass frühzeitig während der **20. Legislaturperiode** ein solches Gesetz parlamentarisch und gesellschaftlich beraten und verabschiedet wird.

Damit kann der deutsche Gesetzgeber Vorbildwirkung innerhalb der Europäischen Union haben. Die normativen und praktischen Defizite beim Beschäftigtendatenschutz sind innerhalb der EU vergleichbar. Letztlich kann eine sachgerechte und ausgewogene nationale Regelung die Blaupause für eine **europäische Regulierung** in diesem Bereich sein, wofür es angesichts der grenzüberschreitenden Verarbeitung von Beschäftigtendaten im Binnenmarkt ein großes Bedürfnis gibt.

[56] Zur Zulässigkeit der Verbandsklage nach EU-Recht vor Geltung der DSGVO implizit EuGH 01.10.2019 – C-673/17 Rn. 32; jetzt Vorlage beim EuGH durch BGH 28.05.2020 – I ZR 186/17; zur UKlaG-Klagemöglichkeit ausführlich Weichert in Däubler u.a., Einleitung UKlaG Rn. 17, § 2 UKlaG Rn. 1 ff.
[57] Weichert in Däubler u.a., Art. 80 Rn. 1a m.w.N.

Literatur

Däubler, Wolfgang, Gläserne Belegschaften, 8. Aufl. 2019.

Däubler, Wolfgang/Wedde, Peter/Weichert, Thilo/Sommer, Imke, EU-DSGVO und BDSG, 2. Aufl. 2020 (Däubler u.a.).

Schuler, Karin/Weichert, Thilo, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, 08.04.2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf (Schuler/Weichert).

Schwarze (Hrsg.: Becker, Ulrich/Hatje, Armin/Schoo, Johann/Schwarze, Jürgen), EU-Kommentar, 4. Aufl. 2019.

Abkürzungen

ABl.	Amtsblatt der EU
Abs.	Absatz
ArbGG	Arbeitsgerichtsgesetz
Art.	Artikel
Aufl.	Auflage
AuR	Arbeit und Recht (Zeitschrift)
BAG	Bundesarbeitsgericht
BB	Betriebsberater (Zeitschrift)
BDSG	Bundesdatenschutzgesetz
BEM	betriebliches Eingliederungsmanagement
BetrVG	Betriebsverfassungsgesetz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BVerfG	Bundesverfassungsgericht
BMAS	Bundesministerium für Arbeit und Soziales
BT-Drs.	Bundestags-Drucksache
BYOD	Bring your own Device
bzgl.	bezüglich
CDU/CSU	Christlich Demokratische Union/Christlich-Soziale Union
DB	Der Betrieb (Zeitschrift)
DFA	Datenschutz-Folgenabschätzung
d.h.	das heißt
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DSGVO	Europäische Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EGMR	Europäischer Gerichtshof für Menschenrechte
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
f/f.	fort-/folgende
GBR	Gesamtbetriebsrat
GG	Grundgesetz
GRCh/GRC	Europäische Grundrechte-Charta
Hrsg.	Herausgeber
IT	Informations- und Kommunikationstechnik
i.S.v.	im Sinne von
JR	Juristische Rundschau (Zeitschrift)
JZ	Juristenzeitung
KBR	Konzernbetriebsrat
K&R	Kommunikation und Recht (Zeitschrift)
LAG	Landesarbeitsgericht
lit.	Buchstabe
MMR	Multimedia und Recht (Zeitschrift)
m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht

o.g.	oben geannte
PC	Personal Computer
PKW	Personenkraftwagen
PM	Pressemitteilung
Rn.	Randnummer
S.	Seite oder Satz
s.o.	siehe oben
sog.	so genannt/e/r
SPD	Sozialdemokratische Partei Deutschlands
StPO	Strafprozessordnung
s.u.	siehe unten
SZ	Süddeutsche Zeitung
TVG	Tarifvertragsgesetz
u.a.	und andere/unter anderem
UKlaG	Unterlassungsklagegesetz
USA	United States of America
usw.	und so weiter
v.	von
v.a.	vor allem
VersR	Versicherungsrecht (Zeitschrift)
VG	Verwaltungsgericht
vgl.	vergleiche
WM	Wertpapier-Mitteilungen (Zeitschrift)
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
zit.	zitiert
ZPO	Zivilprozessordnung