Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Daten nützen - Daten schützen

Der Ratgeber

Beschäftigten-Datenschutz

Zwischen wirtschaftlicher und persönlicher Abhängigkeit und informationeller Selbstbestimmung

2. Auflage

2. Auflage, März 2018

Herausgegeben
vom Landesbeauftragten
für den Datenschutz und die Informationsfreiheit
Dr. Stefan Brink
Mitautorin: Sabrina Schwab
Königstraße 10a, 70173 Stuttgart
Telefon 0711/615541-0
https://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Bildnachweise Umschlag-Vorderseite:
Joelle M, Maksim Kabakou, Jürgen Fälchle,
alle bei fotolia.com

LfDI: Daten nützen – Daten schützen

Der Ratgeber

Beschäftigtendatenschutz: Zwischen wirtschaftlicher und persönlicher Abhängigkeit und informationeller Selbstbestimmung

Inhaltsverzeichnis

Die Arbeitswelt und somit auch der Beschäftigtendatenschutz betreffen fast jeden von uns, ob auf Seiten der Wirtschaft als Arbeitgeber*in oder auf der anderen Seite als Arbeitnehmer*in.[1] Die jährliche Arbeitszeit beträgt im Durchschnitt 1.552 Stunden.[2] Viel Zeit, um als Arbeitnehmer eine Flut an personenbezogenen Daten zu hinterlassen und als Arbeitgeber, diese persönlichen Informationen zu sammeln.

Die vorliegende Handreichung gibt einen Überblick über die Problemschwerpunkte des Beschäftigtendatenschutzes im privaten Bereich, wie sie an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) herangetragen werden und zeigt die zulässige Verwendung personenbezogener Daten von Beschäftigten anhand von Praxisfällen auf. Lehrbücher zu dieser Materie gibt es zur Genüge. Der Fokus liegt hier vielmehr auf der täglichen Arbeit des LfDI BW im Bereich des Beschäftigtendatenschutzes: echte Beratungsanfragen und eingehende Beschwerden – und echte Lösungen.[3]

Die ab dem 25. Mai 2018 zur Anwendung kommende Datenschutzgrundverordnung[4] lässt das Thema Beschäftigtendatenschutz trotz der Öffnungsklausel in Art. 88 Abs. 1 DSGVO nicht unberührt. Grund genug diesen Ratgeber auf den neusten Stand zu bringen!

A. Der Weg vom Volkszählungsurteil bis zur verfassungskonformen gesetzlichen Regelung

Wie die vergangenen Jahre gezeigt haben, war der Weg des Gesetzgebers zu einem eigenständigen Beschäftigtendatenschutz nicht gerade kurz – und er ist eigentlich noch immer nicht am Ziel angekommen.

Das allbekannte Volkszählungsurteil des Bundesverfassungsgerichts[5] aus dem Jahr 1983 hat mit dem erstmals als Grundrecht bezeichneten Recht auf informationelle Selbstbestimmung den Grundstein gelegt: Jeder Einzelne hat das Recht grundsätzlich selbst über die Verwendung mit seinen persönlichen Daten zu bestimmen. Die bis dahin erlassenen Datenschutzgesetze hielten diesen verfassungsrechtlichen Anforderungen nicht stand. Im Jahr 1990 erließ der Bund ein novelliertes Bundesdatenschutzgesetz (BDSG). Bis 2009 hat man sich, trotz seiner großen praktischen Bedeutung, mit einer eigenständigen Regelung für den Arbeitnehmerdatenschutz Zeit gelassen – im Gegensatz zu den Datenschutzgesetzen vieler Länder.[6] Die Praxis musste solange auf die allgemeinen

[1] Es sind stets Personen männlichen und weiblichen Geschlechts gleichermaßen gemeint; aus Gründen der einfacheren Lesbarkeit wird im Folgenden nur die männliche Form verwendet.
[2] Quelle: Institut für Arbeitsmarkt- und Berufsforschung (IAB): Daten zur kurzfristigen Entwicklung von Wirtschaft und Arbeitsmarkt 04/2013, www.iab.de.
[3] Dabei wird die Anonymität der Beschwerdeführer*innen gewahrt.
[4] 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 (Datenschutz-Grundverordnung).
[5] BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83.
[6] Vgl. bspw. § 36 Landesdatenschutzgesetz Baden-Württemberg.

Regelungen des BDSG zurückgreifen. Forderungen nach der Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes wurden erst nach dem Bekanntwerden von Datenschutzskandalen bedeutender deutscher Unternehmen erfüllt. Beschäftigte von Lidl, der Deutschen Bahn oder der Deutschen Telekom mussten erst Opfer unzulässiger Überwachungsmethoden werden, bis die Bundesregierung im Februar 2009 die Arbeit an einem Arbeitnehmer-datenschutzgesetz wieder aufnahm. Resultat war der als „Sofortmaßnahme“ am 1. September 2009 in Kraft getretene § 32 BDSG.

Das in der darauffolgenden Legislaturperiode auf der Agenda stehende ausführliche „Gesetz zur Regelung des Beschäftigtendatenschutzes“ scheiterte an vehementen Protesten von Arbeitgebern und Gewerkschaften.

Wie in der ersten Auflage dieses Ratgebers prophezeit, hat der deutsche Gesetzgeber erneut die Möglichkeit eigenständiger und spezifischer Regelungen verstreichen lassen und ist so den Besonderheiten des Arbeitsverhältnisses als Nähe- und Abhängigkeitsverhältnis nicht gerecht geworden.

Ab dem 25. Mai 2018 ist die EU-Datenschutzgrundverordnung[7] mit ihrer unmittelbaren Bindung anzuwenden. Für die Datenverarbeitung im Beschäftigungskontext hat der europäische Gesetzgeber durch die Öffnungsklausel in Art. 88 Abs. 1 DSGVO den Weg für eigenständige nationale Regelungen geebnet, die jedoch nicht zu einer absoluten Zersplitterung in diesem Bereich führen dürfen. Das Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung[8] – BDSG-neu – übernimmt zwar in § 26 BDSG-neu den derzeit gültigen § 32 BDSG mit wenigen Zusätzen, stellt aber nach wie vor nur einen Minimalkonsens dar. Die seit Jahrzehnten bestehenden Forderungen nach einem eigenständigen Beschäftigtendatenschutzgesetz bleiben noch immer unerfüllt.

Was aber alles neu macht der Mai? Vergleicht man die bisherige Regelung aus § 32 BDSG mit der neuen aus § 26 BDSG-neu, sticht einem zuerst der Umfang ins Auge. Nur weil § 26 BDSG-neu deutlich länger als seine Vorgängervorschrift ist, heißt das leider nicht, dass er gehaltvoller geworden steht. Der neue § 26 Abs. 1 BDSG-neu lautet:

> „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

[7] 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 (Datenschutz-Grundverordnung).
[8] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU).

(Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind."

Einzige Neuerung in § 26 Abs. 1 BDS-neu ist die Erweiterung der Datenverarbeitung zur Ausübung oder Erfüllung kollektivrechtlicher Pflichten. Die seit langem umstrittenen Punkte, insbesondere das Verhältnis von Satz 1 zu Satz 2 oder die Erweiterung vom Anwendungsbereich des zweiten Satzes auf schwerwiegende Pflichtverletzungen neben Straftaten oder eine Ausweitung auf einen bestimmten Personenkreis von möglichen Betroffenen, anstatt der betroffenen Person, hat der Gesetzgeber trotz Kenntnis der Probleme nicht gelöst. Die Streitpunkte bleiben also nach wie vor bestehen. Entscheidender Unterschied ist jedoch, dass nicht das Bundesarbeitsgericht, sondern der Europäische Gerichtshof das letzte Wort hat – auch wenn noch ein paar Jahre ins Land ziehen werden, bis eine gefestigte Rechtsprechung zu erwarten ist.

I. Die Normenvielfalt im Beschäftigtendatenschutz

Auch die DSGVO hält am altbekannten Verbot mit Erlaubnisvorbehalt fest: Die Verarbeitung personenbezogener (Beschäftigten-) Daten ist also grundsätzlich verboten, wenn sie nicht ausdrücklich vom Gesetz erlaubt ist oder eingewilligt wurde.[9]

Nach wie vor ist der Beschäftigtendatenschutz ein Abbild der bestehenden Regelungen im Arbeitsrecht. Auch dort hat es der Gesetzgeber, trotz nachdrücklicher Postulate verschiedenster Lager, nicht geschafft ein einheitliches Arbeitsrecht zu kodifizieren. Die bestehenden datenschutzrechtlichen Regelungen finden sich weit verstreut in verschiedenen Gesetzestexten. Beispielhaft ist § 39 Abs. 8 und 9 Einkommensteuergesetz, wonach der Arbeitgeber die auf der Lohnsteuerkarte enthaltenen Merkmale nur für die Einbehaltung der Lohnsteuer verwenden darf. Für die Verwendung der Sozialversicherungsnummer durch den Arbeitgeber findet sich in § 18f im Vierten Sozialgesetzbuch eine Spezialvorschrift. Da verliert man schnell den Überblick …

[9] Vgl. Art. 6 Abs. 1 DSGVO.

Voraussetzung ist jedoch, dass die nationalen (Spezial-) Vorschriften im Einklang mit der DSGVO stehen. Als europäische Verordnung wirkt sie unmittelbar und muss nicht durch die Mitgliedsstaaten in nationales Recht umgesetzt werden (vgl. Art. 288 Abs. 2 Vertrag über die Arbeitsweise der Europäischen Union - AEUV). Stehen nationale Vorschriften nicht im Einklang mit ihr, genießt sie Anwendungsvorrang. Ziel der Verordnung ist ein EU-weites einheitliches Datenschutzniveau. Neu eingeführte Instrumente, wie der Europäischen Datenschutzausschuss und das Kohärenzverfahren, sollen für eine europaweite einheitliche Durchsetzung des Datenschutzstandards sorgen.

In den Bereichen, in den der europäische Verordnungsgeber den nationalen Gesetzgebern durch die sogenannten Öffnungsklauseln die Möglichkeit zum Erlass eigenständiger Regelungen gegeben hat, ist nicht die DSGVO, sondern das nationale Recht anzuwenden. Beim Fehlen vorrangiger datenschutzrechtlicher Spezialgesetze findet das BDSG-neu als „Auffanggesetz“ Anwendung[10], soweit es im Einklang mit dem höherrangigen EU-Recht steht. Im Unterschied zur bisherigen Subsidiaritätsregelung aus § 1 Abs. 3 BDSG, sind die Anforderungen an spezialgesetzliche Regelungen jedoch gestiegen: Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften des BDSG-neu nur vor, wenn sie einen Sachverhalt, für den das BDSG-neu gilt, abschließend regeln. Andernfalls finden die Vorschriften des BDSG-neu Anwendung. Aus diesem Grund ist eine Reihe von Gesetzesanpassungen nötig geworden, so beispielsweise auch in den sozialrechtlichen Vorschriften. Rechtssicherheit wird man aber auch an dieser Stelle erst durch eine gefestigte Rechtsprechung erhalten.

Bereits die DSGVO stellt in ihrem Art. 88 Abs. 1 klar, dass auch Kollektivvereinbarungen, wozu auch Betriebs- oder Dienstvereinbarungen zählen[11], Rechtsgrundlage für die Verarbeitung personenbezogener Beschäftigtendaten sein können. Der bisher etwas umständliche Weg, die Betriebsvereinbarungen und sonstige Kollektivvereinbarungen als andere Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG einzuordnen, ist künftig nicht mehr notwendig. Diese Klarstellung findet sich auch explizit in § 26 Abs. 4 BDSG-neu. Der Hinweis auf Art. 88 Abs. 2 DSGVO ist insoweit nur deklaratorisch. Machen die Mitgliedsstaaten oder die Kollektivparteien von Ihrer Möglichkeit aus Art. 88 Abs. 1 DSGVO Gebrauch und erlassen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, müssen diese Vorschriften den Vorgaben des Art. 88 Abs. 2 DGVO entsprechen. Sie müssen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen.[12] Wenn die DSGVO von Grundrechten spricht, zählt hierzu neben dem uns bekannten, vom Bundesverfassungsgericht entwickelten, Grundrecht auf informationelle Selbstbestimmung, das europäische

[10] Vgl. § 1 Abs. 2 BDSG-neu.
[11] Vgl. Erwägungsgrund 155 DSGVO.
[12] Vgl. Art. 88 Abs. 2 DGVO.

Pendant, nämlich Art. 8 GR-Charta[13]. Gemäß Art. 8 Abs. 1 GR-Charta hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

Praxistipp:

Ohne Kenntnis der verstreuten arbeitsrechtlichen Vorschriften ist eine datenschutzrechtliche Bewertung nicht möglich. Arbeitgeber sollten bei der Auswahl betrieblicher Datenschutzbeauftragten auch auf arbeitsrechtliche Fachkenntnisse Wert legen und in spezielle Fortbildungen und Schulungen zum Beschäftigtendatenschutz investieren – fehlt eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, liegt es am Arbeitgeber, sich dieses wertvolle Wissen selbst anzueignen.

DSGVO-Tipp:

Der neue europäische Handlungsrahmen zwingt zu einem Blick über den nationalen Tellerrand. Auch wenn die Rechtsetzung in Sachen Beschäftigtendatenschutz in die Hände der Mitgliedsstaaten und Kollektivparteien gelegt wurde, müssen diese sich an die europäischen Spielregeln halten. Mitspielen kann man aber nur, wer auch die europäischen Grundsätze zum Datenschutz kennt und die europäischen Vorgaben berücksichtigt. Trotz ihrer hohen Anforderungen und Vorgaben, sollte die DSGVO als Chance begriffen werden. Der Schutz der eigenen Daten und damit der Persönlichkeit ist den betroffenen Personen gerade im Beschäftigungsverhältnis ein hohes Anliegen. Unternehmen können sich durch ein gutes Datenschutzmanagement als erstrebenswerten Arbeitgeber verkaufen.

II. Die Regelungen der DSGVO und des BDSG-neu

1. Verarbeitung personenbezogener Daten

Die meisten in der DSGVO verwendeten Begriffe ähneln den uns aus dem BDSG bekannten. Nach wie vor geht es beim Datenschutz um personenbezogene Daten. Was das bedeutet, erklärt ab dem 25. Mai 2018 nicht mehr § 3 Abs. 1 BDSG, sondern Artikel 4 Nr. 1 DSGVO: Personenbezogene Daten sind alle Informationen,

[13] Charta der Grundrechte der Europäischen Union.

die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Diese Person nennt die Verordnung die „betroffene Person“. Beispielhaft sind Adressdaten, Geburtsdaten, Bankverbindungsdaten, Familienstand, Steuer-ID, Telefonnummern und E-Mail-Adressen zu nennen, aber auch Bewerbungen, erbrachte Arbeitszeiten, Krankheits- und Urlaubstage, sind personenbezogene Daten.

Man könnte es sich extrem leicht machen, indem man als Arbeitgeber Datenverarbeitung ohne Personenbezug vornimmt, also mit anonymisierten Daten arbeitet. Sicherlich ist das nicht immer möglich. Aber dort, wo es geht, sollten personenbezogene Daten anonymisiert oder aggregiert werden. Unter aggregierten Daten versteht man die Zusammenfassung von Einzelangaben. Entscheidend ist jedoch, dass die Information nicht auf den Einzelnen rückführbar ist, also nicht auf diesen „durchschlägt“.[14] Sind personenbezogene Daten derart verändert, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können, spricht man von anonymisierten Daten.[15] Und bei diesen Daten ist der Arbeitgeber von der Last der datenschutzrechtlichen Bestimmungen befreit.

Praxistipp:

Um der Gefahr von Datenschutzverstößen und der Sanktion mit Bußgeldern zu begegnen, sollte immer geprüft werden, ob die verfolgten Zwecke nicht auch mit anonymisierten bzw. aggregierten Daten (zusammen-gefassten Daten ohne Bezug zu einzelnen Personen) erreicht werden kann.

Dies ist spätestens mit der Anwendung der DSGVO ab dem 25. Mai 2018 noch wichtiger: Ab dann müssen Arbeitgeber bei bestimmten Rechtsverstößen mit Bußgeldern in Höhe von bis zu 4% des Jahresumsatzes ihres Unternehmens bzw. 20 Millionen Euro Strafe rechnen.

Wie auch die Datenschutzrichtlinie unterscheidet die DSGVO im Gegensatz zum bisherigen BDSG nicht zwischen dem Erheben Verarbeiten oder Nutzen personenbezogener Daten. In Art. 4 Nr. 2 DSGVO werden verschiedene Verwendungsarten personenbezogener Daten unter den einheitlichen Begriff der Verarbeitung gefasst. Das heißt jedoch nicht, dass unter verschiedenen Verarbeitungsmodalitäten nicht die am eingriffsschwächsten auszuwählen ist.

[14] BAG, NZA 1995,185.
[15] Vgl. § 3 Abs. 6 BDSG.

2. Anwendung auf alle Beschäftigten

Um nicht den Rahmen dieser Handreichung durch zahlreiche spezialgesetzliche Regelungen zu sprengen, wird hier nur auf § 26 BDSG-neu und seine Voraussetzungen eingegangen. Diese Norm setzt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zum Zwecke eines Beschäftigungsverhältnisses voraus. Der Begriff des Beschäftigten wird zukünftig in § 26 Abs. 8 BDSG-neu legal definiert. Er ist im Gegensatz zu den engen arbeitsrechtlichen Regelungen sehr weit gefasst und erstreckt sich zur Gewährleistung eines umfassenden Schutzes auf alle möglichen Arbeitsverhältnisse, auf Bewerber ebenso wie auf Azubis oder Zivis.

3. Besonderheiten

Zwei Besonderheiten sind noch zu beachten: Werden Beschäftigtendaten zu anderen Zwecken, also solchen, die nicht mit dem konkreten Beschäftigungsverhältnis verknüpft sind, verarbeitet ist auf die allgemeinen Regelungen der DSGVO, insbesondere auf Art. 6 Abs. 1 lit. f) DSGVO, zurückzugreifen. Das ist etwa der Fall, wenn der Arbeitgeber Pflichten nach dem Geldwäschegesetz oder Anti-Terror-Gesetzen nachkommt – das hat mit dem einzelnen Beschäftigungsverhältnis nichts zu tun.

Ein Grund, warum § 26 BDG-neu im Vergleich zum alten § 32 BDSG länger ist, liegt daran, dass die Regelung besonderer Kategorien personenbezogener Daten direkt in § 26 BDSG-neu selbst und nicht wie bislang in § 28 Abs. 6 bis 8 BDSG erfolgt. Diese Änderung ist aus Gründen der besseren Übersichtlichkeit zu begrüßen. Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person grundsätzlich untersagt, wenn nicht eine der Ausnahmen aus Art. 9 Abs. 2 DSGVO gegeben ist. Der deutsche Gesetzgeber hat für die besonders schutzbedürftigen Daten von der Öffnungsklausel aus Art. 9 Abs. 2 lit. b) DSGVO Gebrauch gemacht und § 26 Abs. 3 BDSG-neu erlassen. Sind die dortigen Voraussetzungen erfüllt, ist eine Verarbeitung dieser Daten zulässig. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist auch auf der Grundlage von Kollektivvereinbarungen möglich.[16]

[16] Vgl. § 26 Abs. 4 BDSG-neu.

Praxistipp:

Arbeitgeber sollten auf eine geordnete und systematische Sammlung personenbezogener Daten ihrer Bewerber und Beschäftigten achten. Durch datenschutzkonforme Protokollierungs- und Löschkonzepte müssen personen-bezogene Daten bei Auskunftsansprüchen und Berichtigungs- und Löschungsbegehren nicht mühselig zusammengesucht werden, sondern können in Kürze extrahiert und den Betroffenen zugänglich gemacht werden.

DSGVO-Tipp:

Die DSGVO stärkt die Betroffenenrechte und verpflichtet die Verantwortlichen zu umfassenden Informationen. Diese Rechte und Informationen stehen auch den Beschäftigten zu. Arbeitgeber sollten sich also nicht nur auf vermehrte Anfragen von Kunden, sondern auch der eigenen Mitarbeiter einstellen. Dass dabei ein sinnvolles Datenschutzmanagementsystem helfen kann, versteht sich von selbst…

Den betroffenen Personen stehen neben den bekannten Rechten aus dem BDSG, wie dem Recht auf Auskunft (Art. 15 DSGVO) und Löschung (Art. 17 DSGVO) – von der DSGVO auch als „Recht auf Vergessenwerden“ bezeichnet – noch weitergehende Rechte zu. Sie können nunmehr auch die Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie die Datenübertragung ihrer personenbezogenen Daten (Art. 20 DSGVO) verlangen. Zur effektiven Rechtsausübung wurde in bestimmten Fällen die Möglichkeit eingeräumt einer Verarbeitung personenbezogenen Daten zu widersprechen (Art. 21 DSGVO).

4. Umfassender Schutz

Auch weiterhin ist der Anwendungsbereich des Beschäftigtendatenschutzes erheblich ausgeweitet – jede Information über Beschäftigte ist in jeder Form geschützt. Mit § 26 Abs. 7 BDSG-neu hält der deutsche Gesetzgeber an der Vorschrift des § 32 Abs. 2 BDSG fest. Die nationale Sonderregelung des § 26 BDSG gilt auch für die Verarbeitung personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Der Geltungsbereich der DSGVO umfasst ja ansonsten nur den Einsatz von Datenverarbeitungsanlagen bzw. setzt die

geordnete Sammlung der Daten in Dateien voraus.[17] Anders beim Beschäftigtendatenschutz: Hier fallen zum Beispiel auch handschriftlich gefertigte Notizen während eines Bewerbungsgesprächs sowie die alltägliche Informationserhebung durch persönliche Befragung oder eine Übermittlung durch Telefonate in den Anwendungsbereich von § 26 BDSG-neu. Durch die Loslösung von einer automatisierten Verarbeitung können auch die im Arbeitsrecht entwickelten zwingenden Schutzprinzipien berücksichtigt werden – etwa beim Fragerecht des Arbeitgebers und dem damit einhergehenden „Recht zur Lüge" des Beschäftigten, wenn er einem Versuch unzulässiger Informationsbeschaffung ausgesetzt ist. Auch hier hilft ihm die datenschutzrechtliche Regelung.

5. Die Datenschutzgrundsätze

In Art. 5 Abs. 1 DSGVO stellt die DSGVO ihre Datenschutzgrundsätze vor. Die uns durch das BDSG bereits bekannten Prinzipien, nämlich das Verbot mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz, der Grundsatz der Erforderlichkeit mit dem Verbot der Vorratsdatenspeicherung, das Gebot der Datenvermeidung und der Datensparsamkeit sowie das Transparenzprinzip, werden in Art. 5 DSGVO festgeschrieben, neu formuliert, ergänzt und erhalten einen neuen – unvergleichlich hohen – Stellenwert, der sich wie ein roter Faden durch die gesamte Verordnung zieht. Bereits Verstöße gegen die Grundsätze der Verarbeitung können ein nicht zu verachtendes Bußgeld von bis zu 20 Mio. EUR oder bei Unternehmen bis zu 4 % ihres weltweit erwirtschafteten Jahresumsatzes des vergangenen Geschäftsjahres nach sich ziehen.[18] Dass der Verantwortliche nach Art. 5 Abs. 2 DSGVO zur Rechenschaft – Stichwort: Accountability – verpflichtet ist, kommt den Datenschutzaufsichtsbehörden ebenso wie den Betroffenen bei der Durchsetzung ihrer Rechte besonders zu Gute.

DSGVO-Tipp:

Rechenschaft ablegen können Verantwortliche nur, wenn sie Datenverarbeitungen in geeigneter Weise dokumentieren und die technischen und organisatorischen Maßnahmen entsprechend anpassen. Eine mögliche Form des Nachweises ist das Verarbeitungsverzeichnis nach Art. 30 DSGVO. Verantwortliche sollten sich daher gut überlegen, ob sie ein solches nicht auch führen möchten, wenn ihr Unternehmen weniger als 250 Mitarbeiter beschäftigt. Grundsätzlich wird nur derjenige, der über alle Verarbeitungen personenbezogener Daten im Bilde ist, überhaupt in der Lage sein, die Grundsätze einzuhalten. Die Frage des Nachweises stellt sich somit zuerst hinterher und dürfte dann eigentlich auch nicht mehr schwer fallen.

[17] Art. 2 Abs. 1 DSGVO.
[18] Vgl. Art. 83 Abs. 5 lit. a) DSGVO.

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 lit. a) DSGVO

Einer der zentralen Grundsätze ist die Rechtmäßigkeit der Verarbeitung. Danach bedarf jede Verarbeitung personenbezogener Daten einer Einwilligung oder einer sonstigen Rechtfertigung (vgl. Erwägungsgrund 40 der DSGVO). Der Grundsatz umschreibt das uns bereits aus § 4 Abs. 1 BDSG bekannte „Verbot mit Erlaubnisvorbehalt“. Bei dem Grundsatz von Treu und Glauben darf man nicht vorschnell an die Generalklausel aus § 242 BGB denken, denn es gilt ein europäisches Verständnis für die Begriffe zu entwickeln. Die Begriffe Treu und Glauben müssen daher autonom für die DSGVO als europäische Norm ausgelegt werden. Die englische Sprachfassung der DSGVO verwendet den Begriff fairness, so dass man für das deutsche Verständnis wohl eher den Begriff fair zu Grunde legen sollte. Das Wort Transparenz spielt durch die weitreichenden Informationspflichten der Art. 12 bis 14 DSGVO und die Rechte der Betroffenen in den Art. 15 ff. DSGVO eine zentrale Rolle, wenn nicht sogar die Hauptrolle in der DSGVO. Die Verarbeitung muss den Grundsatz der Transparenz wahren, also eine Verarbeitung personenbezogener Daten in einer für die betroffene Person nachvollziehbaren Weise.[19]

b. Zweckbindung (Art. 5 Abs. 1 lit. b) DSGVO)

Der Zweckbindungsgrundsatz besagt, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Der Zweckbindungsgrundsatz ergibt unmittelbar aus dem Grundrecht auf Schutz personenbezogener Daten (vgl. Art. 8 Abs. 2 GR-Charta). Er genießt besondere Bedeutung: Nur wenn vor der Datenverarbeitung feststeht, welcher Zweck des Arbeitgebers erreicht werden soll, lässt sich im Nachhinein beurteilen, ob in zulässiger Weise verfahren wurde. Jedes Abweichen vom festgelegten Zweck stellt eine Zweckentfremdung dar, die nach dem derzeitigen BDSG ihrerseits der rechtlichen Rechtfertigung bedarf – oder eben illegal ist. Die DSGVO lockert den im BDSG strengen Zweckbindungsgrundsatz in gewisser Weise auf, indem sie in Art. 6 Abs. 4 DSGVO eine Verarbeitung zu einem anderen Zweck als dem Ursprungszweck gestattet, wenn eine Zweckkompatibilität zwischen dem alten und dem neuen Zweck gegeben ist. Hier sieht Art. 6 Abs. 4 DSGVO aber strenge Voraussetzungen vor, die erfüllt sein müssen.

[19] Vgl. Erwägungsgrund 39 der DSGVO.

c. Datenminimierung (Art. 5 Abs. 1 lit. c) DSGVO)

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein. Hierunter versteht die DSGVO den Grundsatz der Datenminimierung. Die Beschränkung auf das erforderliche Maß, ist uns aus dem BDSG als sogenannter Erforderlichkeitsgrundsatz bekannt. Der Grundsatz der Datenminimierung ist in den einschlägigen Rechtsnormen der DSGVO enthalten (vgl. Art. 6 Abs. 1 lit. b) bis f) und Art. 9 Abs. 2 lit. b), c), f) bis j) DSGVO) und wird auch in § 26 BDSG-neu fortgeschrieben. Das informationelle Selbstbestimmungsrecht des Beschäftigten ist mit dem Eigentumsrecht (Art.14 Abs. 1 und 2 Grundgesetz – GG), mit der unternehmerischen Freiheit (Art. 12 Abs. 1 GG) und der Vertragsfreiheit des Arbeitgebers (Art. 2 Abs. 1 GG) in einen schonenden Ausgleich zu bringen. Hier stehen sich also immer Grundrechte auf beiden Seiten gegenüber. Daher misst § 26 BDSG die Verwendung personenbezogener Daten am Grundsatz der Erforderlichkeit. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten muss geeignet und zugleich das relativ mildeste Mittel sein, um die unternehmerischen Interessen und Zwecke bei der Durchführung des Beschäftigungsverhältnisses zu verwirklichen. Dementsprechend verpflichtet das Erforderlichkeitsprinzip stets zum Vergleich alternativer Handlungsformen und zwingt den Arbeitgeber zur Datenvermeidung und Datensparsamkeit, wo immer dies möglich ist.[20] Der Beschäftigte muss seine Daten nur dann preisgeben, wenn der Arbeitgeber ohne ihre Kenntnis im konkreten Einzelfall eine legitime Aufgabe nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Gleichzeitig gibt der Arbeitgeber aber durch seine unternehmerische Entscheidungsfreiheit den Zweck und die konkrete Ausgestaltung des Beschäftigungsverhältnisses vor. Entscheidet sich der Arbeitgeber etwa, besonders qualitätsvolle Produkte anzubieten, so darf er das benötigte gut ausgebildete Personal entsprechend intensiver auswählen und bei der Arbeit überprüfen. Der Maßstab der Erforderlichkeit orientiert sich also in erster Linie an der unternehmerischen Entscheidungsfreiheit, die Zwecke des Beschäftigungsverhältnisses zu bestimmen.

Alles was zur Ausübung von Weisungsrechten eines Arbeitgebers oder einer Kontrolle der Leistung oder des Verhaltens seiner Beschäftigten notwendig ist und nach den Grundsätzen des Arbeitsrechts erlaubt ist, muss aus datenschutzrechtlicher Sicht als erforderlich eingestuft werden.[21] Das heißt aber nicht, dass der Arbeitgeber seine Mitarbeiter einer Totalkontrolle unterziehen darf und sie einem ständigen Überwachungsdruck ausgesetzt sein dürfen – hiervor schützt sie ihr Recht auf informationelle Selbstbestimmung.

[20] Vgl. Erwägungsgrund 39 der DSGVO; NK-GA/*Brink*, § 32 BDSG Rn. 6.
[21] Vgl. BT-Drucks. 16/13657, 21; Thüsing, NZA 2009, 865, 867.

d. Richtigkeit (Art. 5 Abs. 1 lit. d) DSGVO)

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

DSGVO-Tipp:

Der Arbeitgeber ist nur zur Ergreifung angemessener Maßnahmen verpflichtet. Was als angemessen angesehen werden darf und dementsprechend von ihm verlangt werden darf, muss im Einzelfall entschieden werden. Da jedoch ein umfassender Schutz des Grundrechts auf Schutz personenbezogener Daten Ziel der Verordnung ist (vgl. Art. 1 Abs. 1 DSGVO) sollte der vertretbare Aufwand nicht unterschätzt werden. Das zeigt insbesondere auch das Recht auf „Vergessenwerden“ aus Art. 17 Abs. 2 DSGVO.

e. Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DSGVO)

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

DSGVO-Tipp:

Um den Grundsatz der Speicherbegrenzung gerecht zu werden, werden Arbeitgeber nicht darum herum kommen konkrete Lösch- und Speicherkonzepte zu erstellen. Diese sind auch Voraussetzung zur Erfüllung ihrer Informationspflichten (vgl. Art. 13 Abs. 2 lit a) und Betroffenenrechte (vgl. Art. 15 Abs. 1 lit d) DSGVO).

f. Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DSGVO)

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Der

Grundsatz soll zum einen vor unbefugter oder unrechtmäßiger Verarbeitung und zum anderen vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung personenbezogener Daten schützen. Hierzu sind angemessene Schutzmaßnahmen zu treffen. Welche das im Einzelfall sein können, konkretisiert Art. 32 DSGVO.

Wie wir bislang in unserer täglichen Arbeit gesehen haben, waren bereits die Grundsätze des BDSG, vielen Unternehmen Grundsätze im schlechtesten Fall völlig fremd oder wurden eher als Empfehlung denn als verbindliche Vorgabe verstanden. An diesem leider weit verbreiteten Irrtum werden – hoffentlich – spätestens die hohen drohenden Bußgelder etwas ändern.

III. Tarifvertrag und Betriebsvereinbarung

Wie bereits erläutert, kann eine Datenverarbeitung auch auf der Grundlage von Kollektivvereinbarungen möglich sein. Der Abschluss von Tarifverträgen und Betriebsvereinbarungen kann das Fehlen eines eigenständigen Beschäftigtendatenschutzgesetzes in gewissem Umfang wettmachen. Gerade deshalb sollten die Vertragsparteien Tarifverträge und Betriebsvereinbarungen als Regelungsinstrument nicht ungenutzt lassen und die Datenverarbeitungen im Unternehmen entsprechend selbst regeln.

Bedauerlicherweise liefen bisher abgeschlossene Betriebsvereinbarungen nicht selten ins Leere. Unklare oder undurchsichtige Regelungen oder ein das BDSG unterschreitendes Schutzniveau führten mitunter dazu, dass Aufsichtsbehörden eine Betriebsvereinbarung als unwirksam betrachten und auf die allgemeine Regelung des § 32 BDSG zurückgreifen mussten.

Die Anforderungen an kollektive Regelungen steigen mit dem 25. Mai 2018 noch weiter: Der Gestaltungsfreiraum von Arbeitgebern und Betriebsräten wird neben dem Schutzauftrag aus § 75 Abs. 2 BetrVG zusätzlich durch Art. 88 Abs. 2 DSGVO begrenzt: Eine Betriebsvereinbarung muss angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen. Dies gilt insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb eines Unternehmensverbunds und Überwachungssysteme am Arbeitsplatz.

Der Schutzauftrag aus § 75 Abs. 2 BetrVG und die Anforderungen aus Art. 88 Abs. 2 DSGVO erlauben keine Absenkung des Datenschutzstandards gegenüber den Beschäftigten. Durch die in Art. 88 Abs. 2 DSGVO definierten Anforderungen ist die bislang teilweise vertretene Ansicht, dass durch Betriebsvereinbarungen auch negativ vom Schutzstandard des BDSG abgewichen werde könne (vgl. . insbesondere die umstrittene Entscheidung BAG 27.5.1986 – BAGE 52, 88 = NZA 1986, 643, 646; differenzierend Wolff/Brink/Bäcker, BDSG, § 4 Rn. 14 f.) endgültig

nicht mehr haltbar. Andernfalls würde auch der Sinn und Zweck der Verordnung – eine Harmonisierung des Datenschutzstandards innerhalb der EU – in Frage gestellt.

Insoweit muss sich jeder Betriebsrat klar machen: Schlecht verhandelte Betriebsvereinbarungen können, wenn sie unter das Datenschutzniveau der DSGVO absinken, die Rechte der Beschäftigten verletzen. Daran sollte kein Betriebsrat mitwirken. Die Betriebsvereinbarung wird dann nicht als Rechtsgrundlage dienen, so dass die allgemeinen Vorschriften des § 26 BDSG-neu heranzuziehen sind. All die Arbeit oft mühseliger Verhandlungen zwischen den Betriebsparteien, hätte keinen Mehrwert gehabt. Hieran wird auch kein Arbeitgeber ein Interesse haben können.

DSGVO-Tipp:

Die gestiegenen Anforderungen machen für die meisten Betriebsvereinbarungen eine Anpassung erforderlich. Wie Arbeitgeber und Betriebsrat dieser Herausforderung begegnen, sei es durch Anpassung jeder einzelnen Betriebsvereinbarung oder dem Abschluss einer Rahmenbetriebsvereinbarung, die für bereits abgeschlossene aber auch für künftig abzuschließende Betriebsvereinbarung Anwendung findet, bleibt den Betriebsparteien überlassen. Fest steht, dass der Handlungsbedarf dringend erkannt werden sollte. Nur die wenigsten Betriebsvereinbarungen werden bspw. die Zwecke der Verarbeitung konkret und bestimmt genug benennen oder die hohen Anforderungen in Sachen Transparenz erfüllen. Aber auch bei der Bestimmung angemessener und besonderer Schutzmaßnahmen im Sinne von Art. 88 Abs. 2 DSGVO wird auf die Betriebsparteien einiges an Arbeit zukommen. Hiervor sollten sie jedoch nicht zurückschrecken, sondern die Möglichkeit nutzen!

Leider führen nicht selten die fehlende Fachkunde im Datenschutz und die Besonderheit eines Arbeitsverhältnisses zu undurchsichtigen Vereinbarungen. Hier sind betriebliche Datenschutzbeauftragte und die Aufsichtsbehörden gleichermaßen gefragt. Sie können der verantwortlichen Stelle, aber auch dem Betriebsrat beratend zur Seite stehen.[22] Nicht auf Anhieb wird die Aufsichtsbehörde als Berater eingeschaltet. Dies kann mit ihrer vermeintlichen Verortung im „feindlichen Lager“ zusammenhängen. Würde jede geplante Betriebsvereinbarung, welche die Verarbeitung personenbezogener Daten zum Gegenstand hat, der zuständigen Aufsichtsbehörde zur Kontrolle vorgelegt werden, würde diese zudem schnell an ihre Beratungsgrenzen stoßen. Durch gezielte Aufklärungsarbeit ist daher ausreichende

[22] Vgl. Art. 57 Abs. 1 lit. d) DSGVO.

Sensibilität für den Datenschutz zu schaffen.[23] Werden Prozesse von Anfang an unter dem Gesichtspunkt datenschutzrechtlicher Vorgaben vorangetrieben, werden Entwicklungen auch nicht ausgebremst, sondern von vornherein transparent und nachhaltig gestaltet. Zukünftig wird die Aufsichtsbehörden noch mehr die Rolle des Beraters einnehmen. Diesen Spagat zwischen Bußgeldbehörde einerseits und Beratungsstelle andererseits gilt es zum Schutz der betroffenen Personen graziös zu meistern.

In der Regel wird der LfDI BW durch Beschwerden von Betroffenen auf unzureichenden Regelungen in Betriebsvereinbarungen aufmerksam. Nicht selten sind bestehende Betriebsvereinbarungen den Beschäftigten selbst überhaupt nicht bekannt. Unternehmen müssen ihre Beschäftigten daher wiederkehrend über die geltenden Regelungen im Unternehmen informieren und ihnen diese jederzeit zugänglich machen.

Auch wenn es um den Schutz des Einzelnen geht, zieht ein Beschwerdeverfahren häufig nicht nur ein positives Ergebnis für den betroffenen Beschäftigten nach sich. Abgestellte Datenschutzverstöße führen oft zur Verbesserung des Datenschutzes für die gesamte Belegschaft. Die Aufsichtsbehörde wechselt die (angeblichen) Fronten und nimmt die Beraterroller ein – nicht selten auch für später geplante Datenverarbeitungsprozesse, bei denen personenbezogene Daten betroffen sind.

Fall 1: Von der unerlaubten Öffnung eines E-Mail-Postfaches zum Abschluss einer Betriebsvereinbarung

Ein ausgeschiedener Mitarbeiter beschwerte sich darüber, dass sein personalisierter E-Mail-Account, *name@unternehmen.de*, nicht unmittelbar nach seinem Ausscheiden gelöscht wurde. Es stellte sich heraus, dass es im Unternehmen keine Regelungen zur Nutzung der Informations- und Kommunikationstechnik (IuK) gab. Die Mitarbeiter gingen davon aus, dass die private Nutzung der betrieblichen IuK gestattet war und wurden auch nicht durch stichprobenartige Kontrollen und daraufhin ausgesprochene Sanktionen vom Gegenteil überzeugt. Als Folge hatte sich die Erlaubnis zur Privatnutzung der IuK durch „betriebliche Übung“ etabliert. Damit war das Unternehmen als Dienstanbieter im Sinne des TKG bzw. TMG anzusehen und dem Fernmeldegeheimnis[24] unterworfen. Der Zugriff auf den E-Mail-Accounts des ausgeschiedenen Mitarbeiters war somit unzulässig. Und dies betraf nicht nur dessen private Mails, sondern natürlich auch seine dienstlichen, denn in seinem Account waren sie nicht auseinanderzuhalten. Ein massives Problem für das Unternehmen!

Wir haben der verantwortlichen Stelle die verschiedenen Regelungsmöglichkeiten samt ihren Konsequenzen aufgezeigt. Von einer Erlaubnis der Nutzung der betrieblichen IuK zu privaten Zwecken raten wir grundsätzlich ab, zumal hiermit

[23] Vgl. Art. 57 Abs. 1 lit. d) DSGVO.
[24] Vgl. § 88 Telekommunikationsgesetz.

erhebliche Nachteile für den Arbeitgeber verbunden sind: Da er von den Aufsichtsbehörden als Dienstanbieter im Sinne des TKG bzw. TMG angesehen wird und damit an das Fernmeldegeheimnis gebunden ist, verliert er die Zugriffsmöglichkeiten auf für den Betrieb wichtige Kommunikationsergebnisse. Hierdurch erschwert er sich die Einhaltung gesetzlicher Dokumentations- und Kontrollpflichten (nach der Abgabenordnung und dem HGB) und macht sich bei der Ausübung seiner Direktions- und Kontrollrechte von der Einwilligung seiner Beschäftigten abhängig.[25] Das Interesse des Arbeitgebers, seinen Mitarbeitern zumindest während der Pausenzeiten die private Nutzung der betrieblichen IuK zu ermöglichen, kann zum Beispiel durch die Einrichtung eines gesonderten W-LAN-Netzwerks gestillt werden. Wichtig ist es, klare und verständliche Regelungen zu treffen, die den Mitarbeiter ausreichend informieren und es ihm erlauben, seine Einwilligung in die Verarbeitung seiner Daten und ggf. die Kontrolle seines Mail-Accounts wirksam zu erklären.

Mit unserer unterstützenden Beratung hat das Unternehmen mit dem Betriebsrat eine entsprechende Betriebsvereinbarung abgeschlossen, auf deren Grundlage die Beschäftigten jetzt wirksam in die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen IuK-Daten einwilligen konnten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat zu dieser Thematik eine „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ veröffentlicht. Sie enthält auch eine Musterbetriebsvereinbarung / Anweisung / Richtlinie und steht unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/02/OH_E-Mail_Internet_Arbeitsplatz.pdf zum Download bereit.

Praxistipp:

Durch den Abschluss von Betriebsvereinbarungen können Arbeitgeber und Betriebsrat notwendige Transparenz für die Verwendung von Beschäftigtendaten schaffen. Auch wenn der Gestaltungsspielraum von Betriebsvereinbarung durch die fehlende Rechtsmacht zur Einschränkung der Rechte der Beschäftigten begrenzt ist, können sie ein geeignetes Regelungsinstrument darstellen. Durch verbindliche Regelungen, wie beispielsweise dem Ausschluss einer Nutzung der personenbezogenen Daten zu Zwecken der Verhaltens- und Leistungskontrolle oder der Vereinbarung von Beweisverwertungsverboten können die gegenläufigen Interessen in einen angemessenen Ausgleich zueinander gebracht werden.

[25] Ausf. dazu *Brink* ZD 2015, 295, 298.

DSGVO-Tipp:

Wie die Rechtsprechung des Europäischen Gerichtshofs für Menschrechte (EGMR, Urt. v. 05.09.2017 – Rs. 61496/08) zur Kontrolle der Internetnutzung gezeigt hat, ist die ausreichende Information der Betroffenen das A und O. Da sich der Europäische Gerichtshof auch bisher an der Rechtsprechung des EGMR orientiert hat, kann davon ausgegangen werden, dass die dort aufgestellten Grundsätze auch auf bei der Anwendung der DSGVO nicht außer Acht gelassen werden dürfen. Arbeitgeber bleibt daher nur zu raten, ihre Beschäftigten mit allen zur Verfügung stehenden Mitteln zu informieren und so für das höchste Maß an Transparenz zu sorgen.

IV. Einwilligung

Lässt sich die Verarbeitung personenbezogener Daten nicht auf gesetzliche Grundlage stützen, bleibt als weitere Datenverarbeitungsgrundlage die Einwilligung, also das vorherige Einverständnis des Betroffenen in die Verwendung seiner Daten.[26] Wird eine Einwilligung parallel zu einem gesetzlichen Erlaubnistatbestand eingeholt, sollte die betroffene Person aus Gründen der Fairness darüber informiert werden, dass eine Verarbeitung ihrer personenbezogenen Daten trotz Widerruf der Einwilligung auf der Grundlage einer gesetzlichen Erlaubnisnorm möglich sein kann. Aber kommt eine Einwilligung im Beschäftigungsverhältnis überhaupt in Frage? Googelt man den Begriff Arbeitnehmer, spuckt die Suchmaschine Folgendes aus:

„Person, die abhängig, nämlich bei einem Arbeitgeber, beschäftigt ist."

Die wirtschaftliche und persönliche Abhängigkeit einer Person legt den Schluss nahe, sie in einer Zwangslage zu sehen, die ihr eine freie Entscheidung unmöglich macht. Diese Annahme führte bei Datenschützern lange Zeit dazu, eine Einwilligung von Beschäftigten grundsätzlich nicht als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung zu akzeptieren. Zu Recht hat man diesen Extremstandpunkt mittlerweile aufgegeben und den Beschäftigten ihr Recht auf informationelle Selbstbestimmung auch in einem Arbeitsverhältnis zugesprochen. Spätestens mit der DSGVO könnte diese Ansicht auch nicht mehr vertreten werden. Der Streit, ob eine Einwilligung auch im Beschäftigungsverhältnis möglich ist, wird durch § 26 Abs. 2 BDSG-neu endgültig beendet. Aus § 26 Abs. 2 BDSG, aber auch aus Art. 6 Abs. 1 lit. a) DSGVO ergibt sich, dass auch einem Beschäftigten eine Einwilligung möglich sein muss. Es liegt nämlich in der Hand jedes Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen – der Arbeitnehmer bestimmt ergo selbst, ob er seinem Arbeitgeber mehr von sich preisgibt, als dieser nach den gesetzlichen Vorgaben

[26] Vgl. Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a) DSGVO und § 26 Abs. 2 BDSG-neu.

befugt wäre zu erfahren. Die Einwilligung kann auch positive Folgen für den einzelnen Arbeitnehmer haben, so dass es mit dem Sinn und Zweck des Datenschutzes nicht vereinbar wäre, die Beschäftigten pauschal der Möglichkeit einer Einwilligung zu berauben.

Das heißt jedoch nicht, dass wir als Aufsichtsbehörde gezwungen sind, Einwilligungen von Beschäftigten ungeprüft als Ermächtigung zur Datenverarbeitung anzuerkennen. Vielmehr sind wir gehalten, die Freiwilligkeit und Wirksamkeit einer jeden Einwilligung einer genauen Einzelfallprüfung zu unterziehen, wie die nächste Falldarstellung veranschaulicht.

Fall 2: Die „freiwillige“ Urinprobe

Der minderjährige Beschwerdeführer befand sich in einem Berufsausbildungsverhältnis.[27] Weil sein Arbeitgeber ihn verdächtigte, Cannabis zu konsumieren, erklärte sich der Beschwerdeführer bereit, sich einem Drogentest zu unterziehen. Der Arbeitgeber sah die Einwilligung als wirksame Rechtsgrundlage zur Verarbeitung der besonderen Arten personenbezogener Daten (Gesundheitsdaten nach § 3 Abs. 9 BDSG bzw. Art. 9 Abs. 1 DSGVO) des Beschäftigten an. Wir mussten ihn jedoch vom Gegenteil überzeugen. Gegen die Wirksamkeit der Einwilligung sprach im vorliegenden Fall neben der mangelnden Freiwilligkeit der Einwilligung und der Minderjährigkeit des Beschwerdeführers auch die Beschäftigung im Berufsausbildungsverhältnis.

Gemäß § 4a Abs. 1 Satz 1 BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien und informierten Entscheidung des Betroffenen beruht. Zukünftig definiert Art. 4 Nr. 11 DSGVO, was unter einer Einwilligung zu verstehen ist: Eine Einwilligung der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Anforderungen an eine wirksame Einwilligung finden sich ab dem 25. Mai 2018 nicht mehr in § 4a BDSG, sondern in Art. 7 DSGVO. Besondere Bedingungen gelten für die Einwilligungen von Kindern in Bezug auf die Dienste der Informationsgesellschaft (vgl. Art. 8 DSGVO).

Da die Einwilligung in Kenntnis der Sachlage gegeben werden muss, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen.[28]

Es reicht nicht aus, nur auf die Einwilligung zu verweisen. Vielmehr sind auch die Umstände, unter denen die Einwilligung abgegeben wird, einzubeziehen.[29] Eine

[27] Zu den Beschäftigten im Sinne des BDSG zählen auch die zu ihrer Berufsausbildung Beschäftigten, vgl. § 3 Abs. 11 Nr. 2 BDSG.
[28] Vgl. vgl. Erwägungsgrund 42 Satz 4 der DSGVO.

Einwilligung beruht auf der freien Entscheidung des Betroffenen, wenn sie ohne Zwang abgegeben wird.[30] Sie kann als Verwendungsregulativ nur so lange akzeptiert werden, wie sich der Betroffene nicht in einer Situation befindet, die ihn faktisch dazu zwingt, sich mit dem Zugriff auf seine verlangten Daten einverstanden zu erklären.

Der Arbeitgeber konnte vorliegend nicht ernsthaft von einer zwanglosen Willenserklärung ausgehen. Allein schon die Tatsache, dass sich der Beschwerdeführer in einer Berufsausbildung befand, lässt an der Freiwilligkeit der Entscheidung zweifeln. Beschäftigte in der Berufsausbildung befinden sich gegenüber dem Arbeitgeber in einer noch unterlegeneren Position, als es ausgebildete Beschäftigte tun. Der Auszubildende ist auf die Vermittlungswilligkeit des Ausbilders angewiesen und ist daher besonders zu schützen.[31]

Die in den Blick zu nehmenden begleitenden Umstände stritten demnach eindeutig für eine unter Zwang und Druck abgegebene Erklärung: Nach Angaben des Arbeitgebers hat der Beschwerdeführer bei der Konfrontation mit dem Verdacht des Drogenkonsums stark angefangen zu zittern und diesen mit widersprüchlichen Antworten zu zerstreuen versucht. Zum Schluss soll der Betroffene den Konsum von Cannabis sogar eingeräumt haben. Es musste auch berücksichtigt werden, dass das Gespräch im Beisein weiterer Mitarbeiter stattgefunden hat. Vermutlich wollte der Arbeitgeber sich so eine eventuell noch notwendig werdende Beweisführung sichern. Die durch die Anwesenheit weiterer Personen wachsende Drucksituation und entstehende Prangerwirkung kann aber nur schlecht geleugnet werden.

Eine freiwillige Entscheidungsfindung scheiterte auch an der Minderjährigkeit des Beschwerdeführers. Ob Minderjährige in die Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten wirksam einwilligen können, beurteilt sich ab der Anwendung der DSGVO nicht mehr nach dem Grad ihrer Einsichtsfähigkeit, sondern nach dem Erreichen des sechzehnten Lebensjahres.[32] Ob bei dieser abstrakten Aussage, von einer Einsichtsfähigkeit gesprochen werden kann, wird sich zeigen. Da der Fall nach der Rechtslage des BDSG entschieden wurde, sprachen die Umstände des Einzelfalls dafür, neben der Einwilligung des Beschwerdeführers auch die seines gesetzlichen Vertreters als notwendig anzusehen, da die Konsequenzen insbesondere in Bezug auf den weiteren beruflichen Werdegang als gravierend anzusehen waren.

Hinzu kam noch, dass die von § 4a Abs. 3 BDSG gestellten Anforderungen an die Einwilligung zur Erhebung besonderer Arten personenbezogener Daten nicht erfüllt waren. Eine Einwilligung muss sich bei dieser Datenkategorie ausdrücklich hierauf beziehen. Hieran wird auch zukünftig festgehalten.[33]

---

[29] Vgl. Art. 7 Abs. 4 DSGVO.
[30] Vgl. Erwägungsgrund 42 der DSGVO
[31] Dies belegt schon die Existenz des Berufsbildungsgesetzes.
[32] Vgl. Art. 8 Abs.1 DSGVO.
[33] Vgl. § 26 Abs. 3 Satz 2, letzter Halbsatz BDSG-neu.

Die Erhebung besonderer Arten personenbezogener Daten war auch nicht nach § 28 Abs. 6 Nr. 3 BDSG erlaubt und wäre es auch nicht nach § 26 Abs. 3 BDSG-neu gewesen. Beide Vorschriften knüpfen die zulässige Datenverarbeitung an das Erforderlichkeitsprinzip. Dass der Arbeitgeber dieses hier grob außer Acht gelassen hat, liegt auf der Hand. Der Beschwerdeführer hatte ja seinen Cannabiskonsum selbst bestätigt; auf Nummer sicher gehen musste der Arbeitgeber daher alle mal nicht, ein weiterer Test war überflüssig.

In diesem Zusammenhang ließen wir es uns nicht nehmen, Hinweise zur Durchführung von Drogentests im Allgemeinen zu geben: Sie sind nur zulässig, wenn Beschäftigte hierzu schriftlich wirksam eingewilligt haben. Der Test muss darauf gerichtet sein, eine Alkohol- oder Drogenabhängigkeit nachzuweisen. Es darf nicht lediglich darum gehen, den Alkohol- oder Drogenkonsum zu ermitteln. Nichts anderes macht aber ein THC-Schnelltest. Er trifft keinerlei Aussage über die physische oder psychische Verfassung des Betroffenen, die eine Drogenabhängigkeit belegen könnte. Noch wichtiger: Ein solcher Test muss erforderlich sein, um die Eignung des Arbeitnehmers für die konkret vorgesehene Tätigkeit festzustellen. Arbeitsplatzrelevantes Verhalten liegt allerdings nur vor, wenn der Mitarbeiter durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte des Arbeitgebers gefährden könnte. Ob der Drogenkonsum strafbar wäre oder nicht, ist nicht die Sache des Arbeitgebers. Dem Arbeitgeber darf zudem nur das Ergebnis der Eignungsuntersuchung vom untersuchenden Arzt mitgeteilt werden, nicht eine nähere Diagnose oder einzelne Gesundheitszustände.

Praxistipp:

Die Einwilligung des Beschäftigten kann nur dann als Rechtsgrundlage für die Verwendung seiner Daten dienen, wenn die hohen gesetzlichen Anforderungen – Transparenz, Freiwilligkeit, Schriftform – eingehalten werden. Das Argument der Zwangslage und Unfreiwilligkeit kann der Arbeitgeber minimieren, indem er die Einwilligung an die Gewährung rechtlicher Vorteile knüpft, auf die der Betroffen sonst keinen Anspruch hätte.

DSGVO-Tipp:

Auch wenn der Streit, ob eine Einwilligung auch im Beschäftigungsverhältnis möglich ist, durch Art. 6 Abs. 1 lit. a) DSGVO und § 26 Abs. 2 BDSG-neu endgültig beendet wurde, besteht auch weiterhin das gleiche Problem: Nach wie vor sind an die Beurteilungen der Freiwilligkeit strenge Anforderungen zu stellen. Zusätzlich zu den Anforderungen aus Art. 7 DSGVO, muss nach § 26 Abs. 2 BDSG-neu insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, berücksichtigt werden. Nach dem Willen des Bundesgesetzgebers kann Freiwilligkeit insbesondere dann vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Ein rechtlicher oder wirtschaftlicher Vorteil liegt beispielsweise bei der Gestattung der dienstlichen Informations- und Kommunikationstechnologie zur privaten Nutzung. Von der Verfolgung gleichgelagerter Interessen kann insbesondere bei der Durchführung eines betrieblichen Eingliederungsmanagements ausgegangen werden (vgl. BT-Drs 18/11325, S. 97). Anders als von der DSGVO vorausgesetzt, muss die Einwilligung schriftlich erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (vgl. § 26 Abs. 2 DSGVO). Mit dem Schriftformerfordernis hat der nationale Gesetzgeber den Anforderungen, die Art. 88 Abs. 2 DSGVO aufstellt, Rechnung getragen. Zusätzlich hat der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 DSGVO in Textform aufzuklären.

B. Die Welt des Beschäftigtendatenschutzes aus Sicht des LfDI BW

Praxisfälle aus der täglichen Arbeit der Aufsichtsbehörden bringen die bestehenden Defizite im Bereich des Datenschutzes ans Licht. Gerade der Bereich des Beschäftigtendatenschutzes stellt sich hier als besonders spannende Rechtsmaterie dar. Oft handelt es sich um brisante Fälle, bei deren Meldung der betroffene Arbeitnehmer Konsequenzen für sein Arbeitsverhältnis befürchtet. Vermutlich finden sich in keinem anderen Bereich des Datenschutzes so zahlreiche anonyme Beschwerden oder der Wunsch der Betroffenen, gegenüber dem Arbeitgeber unerkannt zu bleiben. Auf der anderen Seite birgt das Arbeitsverhältnis als höchstpersönliches Näheverhältnis die latente Gefahr, doch als derjenige ausfindig gemacht zu werden, der bei der Aufsichtsbehörde eine Beschwerde eingereicht hat. Bei Unternehmen mit wenigen Beschäftigten erklärt sich dies von selbst; bei Beschwerden, bei denen der Betroffenenkreis von vornherein durch den dargestellten Sachverhalt begrenzt wird, könnten Nachforschungen Rückschlüsse auf die Person des Beschwerdeführers zulassen.

Dem Wunsch der Betroffenen, ihre Beschwerde nicht gegenüber dem Arbeitgeber zu offenbaren, kommen wir als Aufsichtsbehörde selbstverständlich gerne nach. Wir sind rechtlich in der Lage, Nachfragen des Arbeitgebers zur Identität eines Beschwerdeführers zurückzuweisen. Zugleich sprechen wir aber mit dem Beschwerdeführer über die Möglichkeit des Arbeitgebers, Rückschlüsse auf seine Identität auch bei einer anonymen Vorgehensweise zu ziehen.

I. Der Weg ins Beschäftigungsverhältnis

Viele kennen das: Mühselig werden alle Bewerbungsunterlagen zusammengesucht, ein freundliches Foto, für das ein überteuerter Fotograf aufgesucht wurde, gut sichtbar auf das Deckblatt der Bewerbungsmappe geklebt. Hat man letzteres weggelassen, sinkt die Wahrscheinlichkeit, zu einem persönlichen Gespräch eingeladen zu werden, gegen Null.

Jeder Arbeitgeber möchte möglichst aussagekräftige Informationen über zukünftige Mitarbeiter, über ihre fachliche Qualifikation, ihren Werdegang, ihre persönlichen Verhältnisse, ihren Gesundheitszustand und ihre Zukunftsplanung erhalten. Welcher Unternehmer möchte schon einen mehrfach straffällig gewordenen, alleinerziehenden Mitarbeiter, der in der Vergangenheit an häufigen Kurzerkrankungen litt, mit der Aufgabe besonders wichtiger Unternehmensinteressen betrauen? Liegt die Verurteilung wegen Beleidigung des Nachbarn als Ursache einer schief geschnittenen Hecke aber mehr als 20 Jahre zurück und ist der Bewerber Vater eines 17 Jahre alten Kindes, sieht die Sache doch wieder ganz anders aus. Wenn die Kurzerkrankungen einmal eine Migräne, einmal ein Infekt, ein anderes Mal eine Erkältung waren und der Bewerber jeweils zwei Tage arbeitsunfähig

krankgeschrieben war, haben auch diese Informationen ihre Aussagekraft fast vollständig verloren.

Das Interesse von Arbeitgebern nach aussagekräftigen Informationen potentieller Mitarbeiter wird durch das in der Rechtsprechung entwickelte „Fragerecht des Arbeitgebers“ gestillt.[34] Gleichzeitig werden Inhalte und Grenzen dieses Fragerechts durch das „Recht zur Lüge“[35] bei unzulässigen Fragen konterkariert und können auch mithilfe einer Einwilligung nicht erweitert werden. § 32 BDSG sowie künftig § 26 BDSG-neu bindet den Arbeitgeber auch in der Phase vor Begründung eines Beschäftigungsverhältnisses an das Erforderlichkeitsprinzip und nimmt somit Einfluss auf die Konzeption und Durchführung des Auswahlverfahrens. Somit dürfen nur solche Informationen erhoben werden, die – je nach Stand des Bewerbungsverfahrens – für die Entscheidungsfindung tatsächlich benötigt werden.

1. Fall 3: Zuviel gefragt!

Immer wieder erreichen uns Beschwerden, bei denen Bewerber unzulässigen Fragen des Arbeitgebers ausgesetzt sind. Bezüge zur konkreten Tätigkeit fehlen nicht selten vollständig. Oft werden uns Personal- und Bewerberbögen vorgelegt, die der Betroffene im Rahmen seiner Bewerbung ausfüllen soll. Hierbei stoßen wir immer wieder auf die nachfolgend dargestellten Fragen:

- Familienverhältnisse

Fragen zu den Familienverhältnissen eines Bewerbers (z.B. Familienstand, alleinerziehend, Zahl und Namen der Kinder) sind grundsätzlich unzulässig. Erkundigungen nach Zahl und Alter der Kinder können ausnahmsweise dann zulässig sein, wenn die Position, für die sich der Arbeitnehmer bewirbt, regelmäßig mit unvorhersehbaren Einsätzen zu ungewöhnlichen Zeiten verbunden ist, die einem alleinerziehenden Elternteil minderjähriger Kinder nicht oder nur schwer möglich sind. Die Frage ist daher nur in besonderen Ausnahmefällen zulässig.

- Stammdaten

Name, Anschrift, Telefonnummer und E-Mail-Adresse sind für den Arbeitgeber erforderlich, um mit dem Bewerber Kontakt aufnehmen zu können. Es reicht aus, wenn der Bewerber beim Arbeitgeber eine Kontaktmöglichkeit angibt. Entsprechend des Stellenprofils kann die Angabe mehrerer Kontaktmöglichkeiten jedoch erforderlich sein, wenn der Bewerber kurzfristig erreichbar sein muss, etwa als Pressesprecher. Regelmäßig nicht zur Identifizierung des Bewerbers notwendig sind Geburtsort, Geburtsname, Alter und Nationalität. Solche Fragen können Indizien für eine Diskriminierung sein.[36] Allerdings besteht die Möglichkeit für den Arbeitgeber,

[34] Vgl. auch BAG 22.10.1986 – 5 AZR 660/85 – DB 1987, 1048.
[35] BAG AP Nr. 2 zu § 123 BGB, st. Rspr.
[36] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 387.

sich im Rahmen des Vorstellungsgespräches den Personalausweis des Bewerbers zur Identifizierung vorlegen zu lassen – damit ist aber nicht gesagt, dass eine Kopie hiervon zulässig ist.

- Fahrerlaubnis

Das Vorhandensein einer Fahrerlaubnis ist nur relevant, wenn diese zur Erledigung der geschuldeten Arbeit benötigt wird.

- Fremdsprachen

Nach Sprachkenntnissen darf gefragt werden, wenn diese für die vorgesehene Tätigkeit bedeutsam sind. Das Ziel, eine gute Kommunikation mit Kunden und Kollegen zu gewährleisten, kann die Frage nach ausgezeichneten oder sehr guten Sprachkenntnissen rechtfertigen.

- Vorstrafen und laufende Ermittlungen

Nach Vorstrafen darf ein Arbeitgeber nur unter Beschränkung auf das für den jeweiligen Arbeitsplatz wichtige Strafrechtsgebiet fragen. Als einschlägig anzusehen sind dabei Vorstrafen, die nach der Art ihrer Begehung oder den betroffenen Rechtsgütern objektiv eine besondere Nähe zu der vorgesehenen Beschäftigung aufweisen. Das Bundesarbeitsgericht hat insoweit zwischen Vermögensdelikten (Bankkassierer), Verkehrsdelikten (Berufskraftfahrer), politischen Delikten (Mitarbeiter des Verfassungsschutzes) und Sittlichkeitsdelikten (Jugendpfleger) unterschieden. Der Arbeitgeber muss daher differenziert vorgehen. Ein einzustellender Busfahrer darf nach Verkehrsdelikten gefragt werden, nicht aber nach begangenen Vermögensdelikten. Vorstrafen, die gemäß § 32 Abs. 2 des Bundeszentralregistergesetzes (BZRG) nicht in ein Führungszeugnis aufgenommen werden, der Tilgung unterliegen oder nur in ein Führungszeugnis für Behörden aufgenommen werden, brauchen gemäß § 53 Abs. 1 BZRG nicht offenbart zu werden, worauf der Bewerber hinzuweisen ist. Grob rechtswidrig ist es, den Bewerber eine Selbstauskunft aus dem BZRG vorlegen zu lassen.

Die Frage nach laufenden Straf- und Ermittlungsverfahren ist zulässig, soweit ein solches Verfahren bereits Zweifel an der persönlichen Eignung und Zuverlässigkeit des Bewerbers für den konkreten Arbeitsplatz begründen kann oder die Verfügbarkeit des Bewerbers durch das Verfahren erheblich eingeschränkt ist, weil mit umfangreichen Ermittlungen, Untersuchungshaft oder der Verurteilung zu einer Freiheitsstrafe zu rechnen ist.

DSGVO-Tipp:

Wie Art. 10 DSGVO zeigt, bleibt das Verlangen von Arbeitgebern nach Auskunft und die Nutzung personenbezogener Daten über Vorstrafen auch ab der Anwendung der DSGVO gewohnt schwierig. Auch zukünftig besteht kein allgemeines Fragerecht des Arbeitgebers bzgl. des Vorliegens strafrechtlicher Verurteilungen. Bereits der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c) und das nationale Pendant hierzu – der Erforderlichkeitsgrundsatz aus § 26 Abs. 1 Satz 1 BDSG-neu – setzt ein tätigkeitsbezogenes Fragerecht voraus.

- Pfändungen und Lohnabtretungen

Bei der Besetzung von Vertrauenspositionen, mit denen beträchtliche finanzielle Spielräume verbunden sind, kann sich der Arbeitgeber erkundigen, ob der Bewerber in geordneten wirtschaftlichen Verhältnissen lebt oder überschuldet ist, ob Lohnpfändungen oder -abtretungen erfolgt sind, der Bewerber eine eidesstattliche Versicherung abgegeben hat oder ein privates Insolvenzverfahren eröffnet wurde. Das gilt allerdings nicht für die Kassiererin im Supermarkt. Es gibt keine Belege dafür, dass arme Kassierer unehrlicher sind als reiche.

- Chronische Krankheiten und beantragte Kuren

Fragen nach Vorerkrankungen und dem Gesundheitszustand eines Bewerbers betreffend seine Intimsphäre sind nur eingeschränkt zulässig. Der Arbeitgeber darf sich danach erkundigen, ob eine Krankheit oder eine Beeinträchtigung des Gesundheitszustands vorliegt, durch welche die Eignung für die vorgesehene Tätigkeit auf Dauer oder in periodisch wiederkehrenden Abständen eingeschränkt ist. Nach ansteckenden Krankheiten, die zwar nicht die Leistungsfähigkeit beeinträchtigen, jedoch die zukünftigen Kollegen oder Kunden gefährden könnten, darf gefragt werden. Ebenfalls in Erfahrung gebracht werden darf, ob es zum Zeitpunkt des Dienstantritts bzw. in absehbarer Zeit zu einer Arbeitsunfähigkeit, z.B. durch eine geplante Operation, eine bewilligte Kur oder auch durch eine zurzeit bestehende akute Erkrankung, kommen kann.

DSGVO-Tipp:

Nach dem Willen des europäischen Verordnungsgebers ist die Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, wozu auch die Gesundheitsdaten von Beschäftigten gehören, grundsätzlich verboten, wenn nicht eine der Ausnahmen nach Art. 9 Abs. 2 DSGVO vorliegen. Von der Öffnungsklausel aus Art. 9 Abs. 2 lit. b) DSGVO hat der deutsche Gesetzgeber durch § 26 Abs. 3 BDSG-neu Gebrauch gemacht. Hiernach ist die Verarbeitung besonderer Kategorien personenbezogener Daten 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 wenn die Verarbeitung dieser besonders schützenswerten Daten ebenso auf eine Einwilligung der Beschäftigten gestützt werden kann (vgl. § 26 Abs. 3 Satz 2 BDSG-neu), wird es in Bewerbungssituation in der Regel an der fehlenden Freiwilligkeit der Einwilligung scheitern. Eine andere Beurteilung ist jedoch für Bewerber für den öffentlichen Dienst möglich. Hier legt das Recht der Schwerbehinderten in SGB IX dem öffentlichen Arbeitgeber besondere Pflichten auf. Bspw. müssen schwerbehinderte Bewerber, deren fachliche Eignung nicht offensichtlich fehlt, zum Vorstellungsgespräch eingeladen werden. Daher kommt es nicht selten vor, dass Bewerber mit einer Schwerbehinderung oder ihnen gleichgestellte ihren Bewerbungsunterlagen entsprechende Nachweise unaufgefordert beilegen.

Praxistipp:

Arbeitgeber müssen sich vor der Ausschreibung einer vakanten Stelle über die mitzubringenden Qualifikationen und das Anforderungsprofil des Bewerbers im Klaren sein. Bewerberinformationen dürfen nicht nach Belieben erfragt werden, um erst im Nachhinein zu entscheiden, welche dieser Angaben man für die Besetzung der Stelle benötigt.

Nur anhand konkreter Stellenprofile ist es einem Bewerber möglich, sich auf ein Bewerbungsgespräch ausreichend vorzubereiten und abzusehen, welche Informationen über ihn für die ausgeschriebene Stelle von Relevanz sind.

2. Fall 4: Blind-Date? Nicht ohne einen Background-Check!

Die Tage, in denen Arbeitgeber vor Stapeln von Bewerbungsmappen saßen und als erste Informationsquelle nur der Lebenslauf und die beigelegten Nachweise dienten, sind längst gezählt. Ähnlich wie bei einem Blind-Date versuchen Arbeitgeber vor dem ersten Treffen oder bereits der Einladung dazu über Suchmaschinen und soziale Netzwerke so viel wie möglich über den potentiellen Mitarbeiter herauszufinden. Wenn dabei peinliche Partybilder oder im schlimmsten Fall auch hasserfüllte Posts über den alten Chef auftauchen, hat man sich ein Bild gemacht, das durch ein persönliches Kennenlernen und zahlreiche Qualifikationsnachweise schwer zu verrücken sein wird. Manchmal haben Arbeitgeber Lebensläufe vor sich, die so beeindruckend sind, dass sie sich fragen, warum der Bewerber ausgerechnet bei ihrem Unternehmen anfragt. Die Ungläubigkeit und das Misstrauen verleitet nicht selten zu einer Überprüfung – einem sog. Pre-Employment-Screening oder auch Background-Check genannt. Was soll schon ein Bachelor und Master of Engineering mit den Abschlussnoten 1.3, Studienaufenthalten in USA, Skandinavien und Asien sowie mit den dazugehörigen fließenden Sprachkenntnissen in einem 20 Mann Betrieb ernsthaft wollen? Oder aber Arbeitgeber sind mit fragmentarischen Lebensläufen konfrontiert und versuchen die Lücken mithilfe des Internets selbst zu schließen.

Dass Background-Checks in der Welt von Headhuntern und im Human-Ressource Bereich eines Unternehmens leider als Selbstverständlichkeit betrachtet werden, zeigen die eingehenden Beschwerden.

Ein großes Pharma-Unternehmen beabsichtigte im Rahmen von Einstellungsverfahren eine umfassende Überprüfung der Lebensläufe aller Bewerber durchzuführen. Argumentationsgrundlage war, wie nicht anders zu erwarten, das besonders sicherheitsrelevante Aufgabengebiet und die hohe Verantwortung des Unternehmens gegenüber der Bevölkerung.

Der Regierungsentwurf vom 15.12.2010 für ein eigenständiges Beschäftigtendatenschutzgesetz sah hierzu in § 32 Abs. 6 vor:

> „Beschäftigtendaten sind unmittelbar bei dem Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind.“ (BT-Drucks. 17/4230)

Auch wenn diese Regelungen eines eigenständigen Beschäftigtendatenschutzes nur Entwurf blieben, findet sich der Aussagegehalt der vorstehenden Regelung im

derzeit gültigen § 32 BDSG wieder[37] und bleibt auch über den 25. Mai 2018 hinaus bestehen.

Anders als § 4 Abs. 2 BDSG normiert die DSGVO nicht, dass personenbezogenen Daten grundsätzlich beim Betroffenen zu erheben sind. Auch wenn der Direkterhebungsgrundsatz nicht unmittelbar aus der DSGVO abgelesen werden kann, ergibt er sich doch zumindest mittelbar: Art. 5 DSGVO sowie aus Art. 8 GR-Charta verlangen, dass eine Datenverarbeitung nur in erforderlichem Rahmen erfolgen darf. Die Erhebung personenbezogener Daten beim Bewerber selbst hat für diesen ganz wesentliche Vorteile. Es bedeutet nämlich, dass er zum einen weiß, dass der potentielle Arbeitgeber eine Information über ihn haben möchte. Zum anderen hat der Bewerber so im Blick, welche personenbezogenen Daten der Verantwortliche denn nun über ihn bekommen hat, nämlich eben das, was er ihm an Informationen gegeben hat. Außerdem wird auf diese Weise sichergestellt, dass der Bewerber auch selbst entscheiden kann, ob der potenzielle Arbeitgeber überhaupt Informationen über ihn erhält – oder eben nicht. Verweigert er die Antwort, dann ist der Verantwortliche darauf angewiesen, die erstrebten Daten bei Dritten zu erheben. Und der Bewerber weiß ab dem Zweitpunkt der Anfrage bei ihm natürlich, dass der Verantwortliche „auf der Pirsch ist“ und kann selbst darüber wachen, dass dieser bei seiner Informationssuche über ihn nicht zu weit geht. Die Informationspflichten des Verantwortlichen wurden im Vergleich zu § 4 Abs. 3 oder § 33 BDSG erheblich erweitert. Sie ergeben sich aus Art. 13 DSGVO, wenn eine Erhebung bei der betroffene Person stattfindet und aus Art. 14 DSGVO, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. Wie auch bisher muss die betroffene Person über die Identität der verantwortlichen Stelle informiert werden. Hier schreibt die DSGVO detailliert vor, dass der Name und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters anzugeben sind (vgl. Art. 13 Abs. 1 lit a), Art. 14 Abs. 1 lit. a) DSGVO). Neu ist, dass auch die Kontaktdaten des Datenschutzbeauftragten weiterzugeben sind, sofern ein solcher bestellt wurde. Der Wortlaut von Art. 13 Abs. 1 lit b) und Art. 14. Abs. 1 lit b) „gegebenenfalls“ ist an dieser Stelle missverständlich. Wie auch bisher muss über die Zwecke der Verarbeitung unterrichtet werden. Hinzugekommen ist aber, – und das dürfte den ein oder anderen Verantwortlichen vor gewisse Herausforderungen stellen – dass auch die Rechtsgrundlage für die Verarbeitung benannt werden muss (vgl. Art. 13 Abs. 1 lit. c) bzw. Art. 14 Abs. 1 lit. c) DSGVO). Ebenfalls bleibt abzuwarten, wie sich die Verantwortlichen in der Erfüllung von Art. 13 Abs. 1 lit. f) DSGVO schlagen werden. Hier verlangt der Verordnungsgeber, dass der Verantwortliche der betroffenen Personen seine oder die berechtigten Interessen eines Dritten mitteilt, wenn die Verarbeitung auf Art. 6 Abs. 1 lit. f) DSGVO beruht. Hierdurch wird der Verantwortliche gezwungen sich zunächst überhaupt einmal darüber Gedanken zu machen, was seine oder die Interessen eines Dritten sind. Im Gegensatz zum BDSG macht die DSGVO keine Einschränkung über die Verpflichtung zur Mitteilung über die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten,

[37] NK-GA/*Brink*, § 32 BDSG Rn. 20.

wenn bereits bei der Erhebung feststeht, dass diese personenbezogene Daten erhalten sollen (vgl. Art. 13 Abs. 1 lit. e) bzw. Art. 13 Abs. 1 lit. e) DSGVO. Es kommt nicht mehr darauf an, ob der Betroffene nach dem Umständen des Einzelfalls mit einer Übermittlung seiner Daten an Kategorien von Empfängern rechnen muss (vgl. § 4 Abs. 3 Satz 1 Nr. 3 BDSG). Die DSGVO geht noch einen Schritt weiter und verpflichtet auch zur Mitteilung über eine Übermittlung personenbezogener Daten über den Geltungsbereich der DSGVO hinaus (vgl. Art. 13 Abs. 1 lit. f) bzw. Art. 14 Abs. 1 lit. f) DSGVO).

DSGVO-Tipp:

Auch wenn der Direkterhebungsgrundsatz nicht mehr ausdrücklich in der DSGVO normiert ist, ergibt sich jedoch mittelbar aus ihr und dem Grundrecht auf Datenschutz. Arbeitgeber sollten auch nach wie vor eine Erhebung beim Betroffenen selbst wählen. Tun sie dies nicht, hat das zur Konsequenz, dass sie der weitreichenden Informationspflicht aus Art. 14 DSGVO nachkommen müssen.

Arbeitgeber dürfen Informationen, die vom Fragerecht nicht erfasst sind, auch nicht über allgemein zugängliche Quellen beschaffen. Anders ist dies nur bei Online-Diensten wie den beruflichen Netzwerken XING oder LinkedIn, die Beschäftigte zur Selbstdarstellung nutzen. Sie lassen ausnahmsweise das schutzwürdige Interesse des Bewerbers hinter dem Interesse des potenziellen Arbeitgebers an einer Datenerhebung ohne Mitwirkung des Beschäftigten zurückstehen. Recherchen in sozialen Netzwerken wie facebook oder twitter stellen sich hingegen als datenschutzrechtlich unzulässig dar. Pre-Employment-Screenings sollten auch nicht auf die Einwilligung des Bewerbers als Legitimationsgrundlage gestützt werden. Zumindest aber ist die besondere Situation des Bewerbers in den Blick zu nehmen, die in der Regel dazu führen wird, die von § 4a Abs. 1 BDSG bzw. von Art. 7 Abs. 4 i.V.m. § 26 Abs. 2 BDSG-neu geforderte Freiwilligkeit verneinen zu müssen.

Praxistipp:

Wir empfehlen, auf die Durchführung von Pre-Employment-Screenings zu verzichten. Dem Arbeitgeber stehen genügend Möglichkeiten (bspw. Vorstellungsgespräch, Nachweis von Unterlagen im Original, Assessment-Center) zur Verfügung, um die richtige Personalentscheidung zu treffen.

3. Fall 5: Arbeitgeber unter sich

In einem anderen Fall sah sich ein Arzt und Arbeitgeber infolge eines fehlenden Arbeitszeugnisses in der „Pflicht“, beim vorherigen Arbeitgeber eines Bewerbers nachzufragen. Im Vorstellungsgespräch wurde der Bewerber damit konfrontiert, dass man nun auch wüsste, warum das frühere Arbeitsverhältnis nicht mehr bestehe.

Die Vorgehensweise des Arztes stellt ohne die Einwilligung des Bewerbers einen Verstoß gegen den Grundsatz der Direkterhebung dar. Auch bei der Besetzung von Positionen mit besonderer Verantwortung rechtfertigt die Sorgfaltspflicht des zukünftigen Arbeitgebers keine Arbeitgeberauskunft ohne die Einwilligung des Betroffenen. Abgesehen davon verletzt der ehemalige Arbeitgeber regelmäßig die aus dem Arbeitsvertrag nachwirkende Treuepflicht, wenn er ohne das Einverständnis des Betroffenen Informationen an Dritte weitergibt. Und ein Verstoß gegen die Informationspflicht nach der DSGVO ist dies allemal.

DSGVO-Tipp:

Denken Arbeitgeber weiterhin, dass sie mit ehemaligen Arbeitgebern eine Art arbeitsrechtliche Schicksalsgemeinschaft bilden würden, die sie zur Nachfrage bei diesem berechtigten würden, ist auch der alte Arbeitgeber zur Informationsmitteilung an seinen ehemaligen Beschäftigten verpflichtet.

4. Fall 6: Mit alten Bewerbungsunterlagen zum neuen Job?

Ist der Kampf im Bewerbungsalltag überstanden, stellen sich viele die Frage: Was passiert eigentlich mit meinen Bewerbungsunterlagen? Die meisten wurden vielleicht schon bei der Stellenausschreibung darauf hingewiesen, dass eine Rücksendung von postalisch eingegangen Unterlagen aus Kostengründen nicht erfolgen wird. Werden die Bewerberstapel dann in den hintersten Kellerecken des Unternehmens aufbewahrt oder landen sie am besten ungeschützt in der blauen Tonne, ohne zuvor auch nur einen Aktenvernichter gesehen zu haben? Wie sieht es mit den per E-Mail eingegangen Bewerbungen aus? Werden sie jemals gelöscht oder können sich auch alle nachfolgenden Personaler oder gar die gesamte Belegschaft problemlos ein Bild der vergangenen letzten Bewerberjahre machen?

Die richtigen Antworten auf diese Fragen hängen erst einmal entscheidend davon ab, ob sich Unternehmen und Bewerber für einander entschieden haben und ein Arbeitsverhältnis eingegangen sind oder nicht. Bei einer Einstellung werden die Bewerbungsunterlagen in der Regel Teil der Personalakte. Pauschale Übernahmen dürfen aber nicht erfolgen, sondern nur in dem zur Durchführung des Beschäftigungsverhältnisses dann erforderlichen Umfang.

Hat sich der Kandidat gegen das Unternehmen als seinen zukünftigen Arbeitgeber entschieden oder dieser die Bewerbung der einzigen Frau bevorzugt behandelt und den männlichen Mitstreitern eine Abfuhr erteilt, sind deren Bewerbungsunterlagen unwiederbringlich zu löschen bzw. zu vernichten. Mit der Entscheidung eines bestimmten Bewerbers für eine vakante Stelle ist der Zweck der übrigen Bewerbungsunterlagen – nämlich das Auswahlverfahren – weggefallen und diese somit zu löschen oder dem Bewerber wieder auszuhändigen. Entsprechend ist zu verfahren, wenn eine Bewerbung von sich aus zurückgezogen wird. Fast jede negative Personalentscheidung birgt jedoch die Gefahr eines Anti-Diskriminierungsprozesses wegen Verstoßes gegen das Allgemeine Gleichbehandlungsgesetzes (AGG). Um Schadensersatzforderungen erfolgsversprechend abwehren zu können, benötigen Arbeitgeber häufig die Bewerbungsunterlagen. Ohne sie wird es Arbeitgebern nur schwer möglich sein nachzuweisen, dass ein Bewerber nicht aus Gründen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität benachteiligt wurde.[38] Die Gefahr, einer AGG-Klage ausgesetzt zu werden, besteht aber nicht ewig. Will ein Bewerber eine Benachteiligung wegen eines vom AGG verbotenen Merkmals geltend machen, muss er dies innerhalb der Zweimonatsfrist des § 15 Abs. 4 AGG tun. Der LfDI BW hält eine Speicherung über drei Monate hinaus daher für nicht erforderlich.

Praxistipp:

Um die Löschfrist von drei Monaten für Bewerbungsunterlagen abgelehnter oder nicht mehr interessierter Bewerber auf eine konkrete Stelle, einzuhalten, sollten die Datenverarbeitungsprogramme so konfiguriert werden, dass eine eigenständige Löschung im entsprechenden Turnus erfolgt.

Es gibt aber auch Fälle, bei denen beide Seiten an einer längeren Speicherung bzw. Aufbewahrung der Bewerbungsunterlagen interessiert sind. Solche Konstellationen findet man insbesondere bei weltweit tätigen Konzernen, die laufend neue Stellen ausschreiben, und bei Initiativbewerbungen. Gibt ein Bewerber unmissverständlich zu verstehen, dass er auch an anderen Positionen im Unternehmen interessiert wäre und bei zukünftigen Stellenbesetzungen berücksichtigt werden möchte, dürfen seine Unterlagen auch für längere Zeit gespeichert werden. Oft stellen Unternehmen Bewerbungsportale zur Verfügung, bei denen die Bewerber ihre Unterlagen selbst hochladen und eigenständig bearbeiten und löschen können. Grundsätzlich ist dieses Format zu begrüßen, da es dem Bewerber den weitesten Spielraum über seine Datennutzung gewährt. Voraussetzung ist aber, den Bewerber ausreichend zu

[38] Vgl. § 1 Allgemeines Gleichbehandlungsgesetz.

informieren, wie seine personenbezogenen Daten verarbeitet werden. Hierzu gehört auch eine Mitteilung, wie die Daten übertragen – hoffentlich auch verschlüsselt! – werden.

Stellt ein Unternehmen zum Einreichen der Bewerbung eine Bewerberplattform zur Verfügung, haben die Bewerber oft auch die Wahl, in einen sogenannten Talentpool aufgenommen zu werden. Hierdurch können die Bewerber auch für zukünftig zu besetzende Stellen berücksichtigt werden.

Bei einer bei uns eingegangen Beschwerde gegen eine führende Wirtschaftsprüfungsgesellschaft hatte sich ein Bewerber mit der Aufnahme in den Talentpool einverstanden erklärt. Aber auch die Datensammlung in einen Talentpool kann nicht zeitlich unbegrenzt erfolgen. Eine wirksame Einwilligung setzt auch die Kenntnis der Speicherdauer voraus. In den Datenschutzhinweisen der Wirtschaftsprüfungsgesellschaft lasen wir, dass die Speicherdauer drei Jahre beträgt und jede Kontaktaufnahme zu einer Verlängerung um weitere drei Jahre führt. Um was für eine Kontaktaufnahme es sich handeln musste, wurde den Bewerbern nicht mitgeteilt. So könnte bspw. auch ein Löschungsbegehren nach dieser schwammigen Regelung dazu führen, dass weitere drei Jahre gespeichert wird. Solche Fallkonstellationen werden Bewerber bei der Abgabe ihrer Einwilligung mit Sicherheit nicht im Sinn gehabt haben. Durch unsere Beratung konnten wir das Unternehmen davon überzeugen, dass bereits die erstmalige Speicherung von drei Jahren für sich genommen weder im Interesse des Unternehmens noch im Interesse des Bewerbers liegen kann. Auf unsere Frage, welchen Aussagegehalt drei Jahre alte Bewerbungsunterlagen in der heutigen Zeit noch haben können, fand das Unternehmen keine überzeugende Antwort. Schließlich konnte erreicht werden, dass die Unterlagen im Talentpool für einen Zeitraum von einem Jahr gespeichert werden dürfen und nur Kontaktaufnahmen, die mit der Eingehung eines Beschäftigungsverhältnisses im konkreten Zusammenhang stehen, zu einer Verlängerung der Speicherdauer um sechs Monate führen können.

Praxistipp:

Entscheidet sich ein Unternehmen Bewerbungsportale zu nutzen und den Bewerbern die Aufnahme in einen Talentpool zu ermöglichen, sollten die Datenschutzhinweise konkret formuliert werden. Hierbei ist insbesondere auf die jederzeitige Widerrufsmöglichkeit der Einwilligung hinzuweisen.

Vorratsdatenspeicherungen von Bewerbungsunterlagen dürfen nicht das Ziel sein, sondern Seriosität. Sonst setzen sich Unternehmen dem Vorwurf aus, unwirksame Einwilligungserklärungen zu produzieren.

DSGVO-Tipp:

Die Anforderungen an die Datenschutzhinweise sind durch die DSGVO enorm gestiegen. Vieles wird für die meisten Arbeitgeber neu sein und sie dementsprechend vor einige Herausforderungen stellen. Unsere Forderung, dass eine Einwilligung auch die Kenntnis über die Speicherdauer voraussetzt, wurde von der DSGVO sogar noch weiter ausgeweitet: Die DSGVO stärkt die Transparenz der Verarbeitung weiter, indem sie dem Verantwortlichen auch auferlegt über die geplante Speicherdauer oder sofern dies nicht möglich ist über die Kriterien für die Festlegung der Speicherdauer Auskunft zu geben (vgl. Art. 13 Abs. 2 lit. a), Art. 14 Abs. 2 lit. a) DSGVO).

Die Liste der Informationspflichten aus Art. 13 und 14 DSGVO ist lang und wird die Verantwortlichen vor einige Herausforderung stellen.

5. Fall 7: Der Datenschutz und seine Tücken

Es kommt nicht selten vor, dass Betroffene unter dem Mantel des Datenschutzes einen Vorteil erzielen wollen – um eine Verletzung in ihrem Recht auf informationelle Selbstbestimmung geht es da manches Mal gar nicht. Als LfDI BW wird man auch mal instrumentalisiert. Erkennen wir, dass der Datenschutz nur als Vorwand dient, um etwa einem früheren Arbeitgeber Ärger zu machen, weisen wir den Betroffenen entsprechend hierauf hin. Dem einen oder anderen Betroffenen kann es dann auch mal die Sprache verschlagen, wie das nächste Praxisbeispiel zeigt:

Der Betroffene bewarb sich aufgrund eines Vermittlungsvorschlags des Jobcenters bei einem Personaldienstleister. Ganz charmant wurde im Bewerbungsschreiben mitgeteilt, dass er die vorgesehene Tätigkeit nicht ausüben könne und auch nicht zur Einarbeitung bereit sei. Für den Fall, dass man ihn zu einem persönlichen Gespräch einladen möchte, behielt er sich vor, von seinem Rechtsbeistand begleitet zu werden. Zur Krönung legte er seiner Bewerbung einen „Übermittlungswiderspruch“ bei, nach dem es dem Personaldienstleister untersagt sein soll, personenbezogene Daten an Dritte weiterzugeben. Hieran hielt sich der Personaldienstleister zum Nachteil des Bewerbers allerdings nicht. Die Folge war die Kürzung von Sozialleistungen durch das Jobcenter.

Entgegen der Auffassung des Beschwerdeführers durften seine personenbezogenen Daten an das Jobcenter übermittelt werden. Nach dem Sozialrecht ist der Arbeitgeber verpflichtet, den Agenturen für Arbeit auf deren Verlangen hin Auskunft über solche Tatsachen zu geben, die für die Entscheidung über einen Anspruch auf Sozialleistungen erheblich sein können.[39] Da das Jobcenter beim

[39] Vgl. § 57 SGB II.

Personaldienstleister Nachfragen zur Ernsthaftigkeit der Bewerbung gestellt hat, durfte er diese auch beantworten. Der Beschwerdeführer wollte nicht auf Anhieb verstehen, dass sein als „Übermittlungswiderspruch“ deklariertes Schreiben nicht die gesetzlichen Erlaubnistatbestände außer Kraft setzen kann. Datenschutz ist also auch für Beschäftigte kein Wunschkonzert.

Praxistipp:

Nicht selten erfolgen Anfragen der Bundesagentur für Arbeit zu solchen Fällen telefonisch oder per E-Mail. Wir empfehlen den Unternehmen daher, das Auskunftsverlangen der Bundesagentur für Arbeit zu Beweiszwecken entsprechend zu dokumentieren.

DSGVO-Tipp:

Die DSGVO legt den Verantwortlichen eine große Bürde auf, die sogenannte Rechenschaftsplicht aus Art. 5 Abs. 2 DSGVO (Accountability). Die Verantwortlichen sind für die Einhaltung der Datenschutzgrundsätze aus Art. 5 Abs. 1 DSGVO verantwortlich und müssen deren Einhaltung auch nachweisen können. Mit einem durchdachten Datenschutzmanagementsystem können sich Verantwortliche einige Zeit und damit auch Kosten ersparen. An dieser Stelle sollten Unternehmen daher nicht zum Sparfuchs werden.

II. Im Beschäftigungsverhältnis angekommen

Ist der Arbeitsvertrag erstmal unterschrieben und sind die neuen Herausforderungen in Angriff genommen, hinterlässt jeder Arbeitnehmer Tag für Tag seine „Datenspuren“ am Arbeitsplatz. Angefangen beim morgendlichen Stechen der Zeitkarte, dem Einloggen am PC, der noch schnell versendeten Erinnerungs-E-Mail an die Ehefrau, die Wäsche in die Reinigung zu bringen, bis hin zur gefertigten Videoaufnahme bei der genommenen Abkürzung durch die Lagerhalle, um eine Raucherpause einzulegen, obwohl eine Dienstanweisung das Aus-und Einstechen hierfür vorschreibt.

1. Fall 8: Auf Schritt und Tritt

Was ursprünglich zur Positionsbestimmung und Navigation im militärischen Bereich vorgesehen war, hat längst im Arbeitsalltag vieler Beschäftigter Einzug gehalten:

Globale Positionsbestimmungssysteme – kurz GPS. Durch GPS kann der Arbeitgeber jederzeit den genauen Standort seiner Beschäftigten ermitteln. Welche Vorteile diese Technik für Arbeitgeber hat und welche Nachteile die Kehrseite der Medaille für die Beschäftigte mit sich bringt, zeigt folgende anonym eingegangene Beschwerde:

Der Beschwerdeführer ist Mitarbeiter eines Unternehmens, das einen Teil der Firmenfahrzeuge mit einem GPS-Ortungssystem ausgestattet hat. Aufgrund verschiedenster Vorfälle in der Vergangenheit, wie etwa unerlaubte Privatnutzung der Fahrzeuge, überflüssige Parallelfahrten und unnötige Mehrfahrten, sah sich das Unternehmen genötigt, über den aktuellen Stand seiner Fahrzeuge und Mitarbeiter stets up to date zu sein. Das Unternehmen versuchte uns davon zu überzeugen, dass das System für die Fahrzeugeinsatzplanung, der Arbeitszeiterfassung und deren stichprobenartigen Kontrolle, der Zuordnung einzelner Kosten zu bestimmten Projekten, dem Diebstahlschutz und einer ordnungsgemäßen Dokumentation der Dienstfahrten gegenüber dem Finanzamt einfach unabdingbar sei. Unabhängig davon habe fast die gesamte Belegschaft „freiwillig“ in die Nutzung der Ortungssysteme eingewilligt.

Aus unserer Sicht kann der Einsatz eines GPS-Ortungssystems durch das Unternehmen nicht auf die Einwilligung der Beschäftigten gestützt werden, da bei einer flächendeckenden Überwachung nicht von der erforderlichen Freiwilligkeit einer Einwilligung der Beschäftigten ausgegangen werden kann. Die hierzu aufgestellten Grundsätze des Bundesarbeitsgerichts können auch mit der Anwendung der DSGVO weiterhin herangezogen werden.

Die Nutzung von Ortungssystemen, mit denen das Arbeitsverhalten von Beschäftigten dauerhaft kontrolliert wird, ist datenschutzrechtlich unzulässig, da Beschäftigte keineswegs einem permanenten Kontrolldruck ausgesetzt sein dürfen.

Nachstehende Punkte sind daher bei der Einführung und dem Betrieb des Ortungssystems von dem betroffenen Unternehmen zu beachten:

- Schon bei der Planung und Ausgestaltung der Systeme ist der Grundsatz der Datensparsamkeit zu verfolgen: Nur die für die betrieblichen Zwecke wirklich erforderlichen Daten, nicht die überflüssigen, sind zu erheben. Eine routinemäßige Ortung eines Fahrzeugs ist unzulässig, wenn sie unabhängig von den notwendigen Planungen erfolgt. Der Einsatz von Ortungssystemen ist nicht erforderlich, wenn der Aufenthaltsort des Beschäftigten auch direkt bei diesem (etwa durch einen Anruf) erhoben werden kann – Grundsatz der Direkterhebung.
- Die Zweckbestimmung muss klar dokumentiert und gegenüber den Beschäftigten in transparenter Weise kommuniziert werden (vgl. Art. 12 DSGVO). Sie sind insbesondere über den Erhebungszweck und -umfang sowie über die Auskunftsrechte hinsichtlich der gespeicherten Daten zu informieren. Daneben müssen die weiteren Informationenpflichten nach Art.

13f. DSGVO erfüllt werden. Entsprechend den Informationspflichten der DSGVO sind die Beschäftigten, etwa durch eine Benachrichtigung oder eine Leuchtanzeige am Gerät, darüber in Kenntnis zu setzen, wann eine Ortung erfolgt. Ansonsten liegt eine verbotene heimliche Überwachung der Mitarbeiter vor.

- Die Beschäftigten sind über die Regelungen der Zugangsberechtigung zu den gespeicherten Daten sowie der Protokollierung der Speicherung und der Festlegung der Speicherungsdauer der Daten zu informieren.

Praxistipp:

Wenn betriebliche Abläufe es dem Arbeitgeber grundsätzlich erlauben Systeme einzusetzen, durch die eine dauernde Verhaltens- und Leistungskontrolle möglich ist, ist der Arbeitgeber gehalten, eine solche Kontrolle durch Betriebsvereinbarungen oder einseitige verbindliche Regelungen auszuschließen. Der Arbeitgeber hat bereits bei der Wahl des Herstellers auf einen möglichen datenschutzkonformen Einsatz der Geräte zu achten – Stichwort: Privacy by design.

Es sollte nicht in Geräte und Systeme investiert werden, bei denen bspw. keine Zugriffsbeschränkung möglich ist.

DSGVO-Tipp:

Das Prinzip von Datenschutz durch Technikgestaltung (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) findet sich auch in Art. 25 DSGVO. Es ist nicht nur Ausdruck des Grundsatzes von Integrität und Vertraulichkeit, sondern auch Ausfluss des Grundsatzes der Datenminimierung. Bei der Neuentwicklung von Datenverarbeitungsprozessen sollen bereits in der Planungsphase Datenverarbeitungen reduziert und Prozesse entwickelt werden, die mit möglichst wenigen Daten auskommen.

2. Wenn personenbezogene Daten auf Wanderschaft gehen

Es ist eigentlich keine Konstellation denkbar, bei der Mitarbeiterdaten das Unternehmen nicht verlassen. Spätestens, wenn es um Fragen wie Sozialabgaben oder Steuern geht, findet immer eine Übermittlung von Beschäftigtendaten an die zuständigen Behörden statt. Die wirklich brisanten Fälle spielen sich aber im täglichen Beschäftigtenalltag ab. Hierzu zählen die Weitergabe an den rechtlich selbstständigen Mutterkonzern, Veröffentlichungen auf der Firmenhomepage oder auch simple Aushänge am schwarzen Brett eines Unternehmens oder im eingerichteten Intranet. Wie auch die Datenschutzrichtlinie unterscheidet die DSGVO im Gegensatz zum bisherigen BDSG nicht zwischen dem Erheben Verarbeiten oder Nutzen personenbezogener Daten. In Art. 4 Nr. 2 DSGVO werden verschiedenen Verwendungsarten personenbezogener Daten unter den einheitlichen Begriff der Verarbeitung gefasst. Die in Art. 4 Nr. 2 DSGVO aufgelisteten nicht abschließenden Beispiele zeigen, dass die DSGVO von einem weiten Begriffsverständnis ausgeht und „jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ mit einbezieht. Die bislang im BDSG notwendig vorzunehmende Unterscheidung zwischen einer Übermittlung[40] und einer Nutzung[41] muss ab dem 25. Mai 2018 nicht mehr getroffen werden. Das löst jedoch nicht das Problem vieler Verantwortlicher für jede einzelne Verarbeitung personenbezogener Daten eine Rechtsgrundlage zur Hand zu haben.

a. Das Mutter-Tochter-Verhältnis

Die aus Sicht des Datenschutzes als problematisch einzustufende Weitergabe von Beschäftigtendaten innerhalb einer Unternehmensgruppe oder eines Konzerns zeigt einmal mehr, dass ein eigenständiges Beschäftigtendatenschutzgesetz längst überfällig ist. Die zunehmende Verflechtung von Unternehmensstrukturen wird vom Gesetzgeber nicht übersehen. Vielmehr treibt er sie durch Abschluss internationaler Regelungen zur Förderung freier internationaler Märkte voran. So heißt es auch in Art. 1 Abs. 1 DSGVO, wenn die Verordnung nicht nur der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten vorsieht, sondern auch den Schutz zum freien Verkehr solcher Daten. Beim Erarbeiten der datenschutzrechtlichen Bestimmungen hat man aber außer Acht gelassen, dass internationale Entwicklungen auch die Verwendung von Beschäftigtendaten beeinflussen. Die Vorstellung, dass ein Arbeitgeber alleine die Leistungskriterien eines Arbeitsverhältnisses bestimmt, ist überholt. Die meisten Beschäftigten haben nicht mehr nur „einen“ Arbeitgeber. Die gesellschaftlichen Strukturen lassen daher arbeitgeberseitige Weisungs- und Kontrollbefugnisse teilweise auseinanderfallen.

An dieser Stelle kann man es aussprechen: Der Datenschutz hinkt hinterher. Das geltende BDSG kennt kein Konzernprivileg, d.h. jedes eigenständige Unternehmen,

[40] Vgl. § 3 Abs. 4 Satz 2 Nr. 3 BDSG.
[41] Vgl. § 3 Abs. 5 BDSG.

das Teil einer Unternehmensgruppe oder eines Konzerns ist, betrachtet das BDSG als jeweils eigene verantwortliche Stelle. Jeder Austausch zwischen Tochterunternehmen und Mutterkonzern bedarf einer Rechtfertigung – gerade so, als seinen Mutter und Tochter nicht miteinander „verwandt“. Klingt nicht nur unpraktikabel, ist es auch. Konzernen kann daher nur empfohlen werden, Konzernbetriebsvereinbarungen abzuschließen, die eine unkomplizierte Weitergabe von Beschäftigtendaten im Rahmen des Notwendigen erlauben. Gleichzeitig kann das Datenschutzniveau durch transparente Information der Beschäftigten über die Datenübermittlung, eine Selbstbindung an Datenschutzregelungen durch Konzernrichtlinien oder auch durch den Abschluss von Datenübermittlungsverträgen[42] erhöht werden.

Die Ungeeignetheit der aktuellen Regelungen wird ab Mai 2018 glücklicherweise durch die DSGVO relativiert. Der europäische Gesetzgeber betrachtet Konzernunternehmen in der Regel als gemeinsame Verantwortliche, die vertraglich unter anderem festzulegen haben, welches Unternehmen für die Erfüllung welcher Betroffenenrechte zuständig ist.[43]

DSGVO-Tipp:

Auch mit der DSGVO wird kein Konzernprivileg eingeführt. Wie Erwägungsgrund 48 der DSGVO zeigt, können jedoch Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Hierbei bleiben die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland aber unberührt. Wie auch bisher muss es für die Datenweitergabe eine Rechtsgrundlage geben. Hierfür bieten sich Konzernbetriebsvereinbarungen an, wenn sie die strengen Anforderungen aus Art. 88 Abs. 2 DSGVO erfüllen.

[42] Bei fehlender Weisungsbefugnis des Mutterkonzerns gegenüber der Tochtergesellschaft kommt ein Auftragsdatenverarbeitungsvertrag in der Regel nicht in Betracht. Eventuell liegt eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO vor.
[43] Vgl. Art. 26 DSGVO.

b. Fall 9: Know-how hat seinen Preis

Der Bereich Mergers & Acquisitions (M&A) umfasst als Sammelbegriff Transaktionen im Unternehmensbereich wie Fusionen, Unternehmenskäufe, Betriebsübergänge, fremdfinanzierte Übernahmen oder auch Unternehmenskooperationen. Der Wert eines Unternehmens misst sich in erster Linie an seinen Mitarbeitern. Qualifiziertes Personal und das damit verbundene Know-how hat seinen Preis. Da leuchtet es nur ein, dass der potentielle Käufer so viele personenbezogene Informationen wie möglich verlangt, der Firmeninhaber ihm diese auch nur zu gern geben möchte. Zum Glück hat der Beschäftigtendatenschutz bei den Vertragsverhandlungen auch ein Wörtchen mitzureden.

Ein großer PC-Hersteller veräußerte einen Teil seines Betriebs an ein anderes Unternehmen. Von dem Betriebsteilübergang waren 20 Mitarbeiter betroffen, wobei sie die Möglichkeit hatten, einer Übernahme durch das neue Unternehmen zu widersprechen und beim alten Arbeitgeber zu gleichbleibenden Bedingungen weiterbeschäftigt zu werden. Um den von der Übernahme betroffenen Mitarbeitern ein Angebot zu machen, erhielt der Erwerber nach Abschluss einer „Vertraulichkeitsvereinbarung“ Kopien der Arbeitsverträge, alle gehaltsrelevanten Daten sowie Daten zur betrieblichen Altersversorgung, Alter, Betriebszugehörigkeit und Arbeitsort der Beschäftigten.

Auch wenn sich die Mitarbeiter durch ein Angebot des Käufers vielleicht wertgeschätzt fühlen, hätten ihre Daten nicht ohne entsprechendes Einverständnis übermittelt werden dürfen. Dies lag im vorliegenden Fall schon wegen des zugesprochenen Widerspruchsrechts jedes Mitarbeiters klar auf der Hand. Ist ein Mitarbeiter unabhängig von verlockenden Angeboten des Erwerbers nicht an einer Übernahme interessiert, ist die Übermittlung seiner Daten erst Recht nicht erforderlich. Umgekehrt bestehen an der Wirksamkeit der Einwilligung in solchen Fällen keine Zweifel, weil die Beschäftigten ja ein Wahlrecht haben, ob sie bleiben oder gehen wollen.

Praxistipp:

Bei einer einem Unternehmensverkauf vorausgehenden Vertragsverhandlung kann das Erwerberinteresse häufig durch anonymisierte Beschäftigtendaten gestillt werden. Möchte der Erwerber es ganz genau wissen, dann nur mit Einwilligung des Beschäftigten.

c. Der Mitarbeiter als Aushängeschild

Wirft man einen Blick auf den Internetauftritt eines Unternehmens, wird man meistens mit einem sympathischen Lächeln des Kollegiums begrüßt. Ob es sich hierbei tatsächlich um das Personal des Unternehmens oder um extra hierfür engagierte Schauspieler handelt, erkennt der Besucher nicht. Will das Unternehmen nicht Gefahr laufen, die Homepage wegen einer unwirksamen oder widerrufenen Einwilligung eines Mitarbeiters für teures Geld umgestalten zu lassen, investiert es lieber gleich in „Professionelle“. Was sich anfangs für die meisten als unnötige Investition darstellt, kann am Ende unnötige Gerichtskosten einsparen.

Eine nette Homepage allein nützt vielen Unternehmen aber relativ wenig. Idealerweise soll der meist genutzte Kommunikationsfluss unserer Gesellschaft – das Internet – auch für die Knüpfung neuer Geschäftskontakte sorgen und bestehende pflegen. Ein kundenfreundliches Erscheinungsbild lässt sich nach Ansicht der meisten Arbeitgeber am leichtesten mit der Möglichkeit einer direkten Kontaktaufnahme mit dem zuständigen Mitarbeiter erreichen. Der Kunde möchte wissen, mit wem er es zu tun hat und wer sein Ansprechpartner ist. Hierfür findet er auf der Internetseite des Unternehmens meist den Namen, die Telefonnummer und E-Mail-Adresse, die Funktion und nicht selten auch das passende Foto des Mitarbeiters.

Ein kundenorientiertes Erscheinungsbild ist fast immer als berechtigtes Interesse eines Arbeitgebers anzuerkennen. Im Gegensatz dazu darf nicht vergessen werden, dass eine Veröffentlichung von personenbezogenen Daten im Internet von jedermann global abrufbar ist und die gefunden Informationen zu einer Person problemlos mit weiteren im Netz vorhandenen Daten zu Persönlichkeitsprofilen zusammengeführt werden können. Der Arbeitgeber hat daher dafür zu sorgen, seinen Internetauftritt so zu konfigurieren, dass Mitarbeiter nicht ohne weiteres von Suchmaschinen wie Google gefunden werden können. Die Veröffentlichung von Arbeitnehmerdaten im Internet ist nur gerechtfertigt, wenn die vertragliche Tätigkeit auch Beziehungen zu Außenkontakten mit sich bringt und der Beschäftigte als direkter Ansprechpartner fungieren soll. So müssen die Kontaktdaten des angestellten Reinigungspersonals selbstverständlich nicht veröffentlicht werden.

Will ein Unternehmen über Namen, Titel, Funktion und dienstliche Erreichbarkeit hinaus der Öffentlichkeit auch ein Foto des Mitarbeiters präsentieren, führt kein Weg an der Einwilligung des Abgebildeten vorbei.[44] Und diese ist freiwillig und kann jederzeit widerrufen werden.

[44] Vgl. die Sondervorschrift des § 22 Kunsturhebergesetzes.

Praxistipp:

Die Mitarbeiter sollten vor der Veröffentlichung ihrer Daten im Internet ausreichend informiert werden und die Möglichkeit haben, den Umfang mitzubestimmen, wobei das Motto „Weniger ist mehr!“ gilt. Äußern Mitarbeiter Bedenken, weil die Veröffentlichung etwa ein Sicherheitsrisiko nach sich ziehen könnte, ist der Arbeitgeber verpflichtet, entsprechende Schutzmaßnahmen zu treffen – für den betroffenen Einzelfall ggfs. auch von einer Veröffentlichung abzusehen.

Auch hier sind die Mitarbeiter auf die Freiwilligkeit der Einwilligung und ihr Widerrufsrecht hinzuweisen. Machen sie von diesem Gebrauch, ist der Arbeitgeber verpflichtet, die personenbezogenen Daten von der Homepage zu nehmen. Schade, dass das Bundesarbeitsgericht bei seinem Urteil – Az. 8 AZR 1010/13 – nicht die widerrufene Einwilligung zur Entscheidungsfindung herangezogen hat. Vielmehr hält es die Löschung eines Firmenvideos, zu dem der Kläger früher sein Einverständnis erteilte hatte, lediglich wegen fehlender eindeutiger Erklärung, dass das Video auch über die Beendigung des Arbeitsverhältnisses hinaus genutzt werden dürfe, für geboten.

DSGVO-Tipp:

Die Entscheidung des BAG kann ab dem 25. Mai 2018 so keinen Bestand mehr haben. Die vom BAG und den Zivilgerichten entwickelten Grundsätze zum Verhältnis von BDSG und KUG können nicht auf das Verhältnis zwischen Kunsturhebergesetz (KUG) und DSGVO übertragen werden. Zwar bleibt den nationalen Gesetzgeber gemäß Art. 85 Abs. 2 DSGVO die Möglichkeit eigene Regelungen zu erlassen. Veröffentlicht der Arbeitgeber aber Bilder seiner Beschäftigten wird er keine journalistischen oder wissenschaftlichen, künstlerischen oder literarischen Zwecke verfolgen, sondern sein Firmenimage stärken wollen. Hierfür sieht die DSGVO keinen eigenen Regelungsspielraum vor. Die Rechtsprechung des BAG widerspricht Art. 7 Abs. 3 DSGVO, der einen jederzeitigen Widerruf der Einwilligung voraussetzt. Der Arbeitgeber hat gemäß § 26 Abs. 2 Satz 4 BDSG-neu die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Abs. 3 DSGVO in Textform aufzuklären. Im Falle eines Widerrufs sind die personenbezogenen Daten zu löschen, es sei denn eine anderweitige Rechtsgrundlage kommt für die Verarbeitung in Betracht (vgl. Art. 17

d. Fall 10: Immer gut informiert

Ein Dauerbrenner in Unternehmen ist die Verwendung von Beschäftigtendaten, die über das „schwarze Brett“ oder das Intranet veröffentlicht werden. Nicht selten auch über Instant-Messaging-Dienste.

In einer anonymen Beschwerde informierte uns ein Beschäftigter eines weltweit führenden Technologiekonzerns in der Antriebs- und Fahrwerktechnik darüber, dass die Firma es mit dem Datenschutz nicht besonders genau nimmt: So wurden Krankmeldungen und Arbeitsunfähigkeitsbescheinigungen öffentlich und für jedermann sichtbar am „schwarzen Brett“ ausgehängt. Wem der Weg zum schwarzen Brett zu weit war, warf einen Blick in den für alle einsehbaren Arbeitsplan samt Informationen zu krankheitsbedingten Abwesenheiten von Kollegen.

Selbstverständlich ist es den Arbeitgebern ein nachvollziehbares Anliegen, ihre Mitarbeiter über die Abwesenheit von Kollegen zu informieren. Nur wenn die Vertretung weiß, dass sie einspringen muss oder der Gang zum Kollegen im Nachbargebäude nicht lohnt, weil er nicht anzutreffen sein wird, kann ein uneingeschränkter Betriebsablauf sichergestellt werden. Zur Erreichung dieses Ziels muss bei der Veröffentlichung von Arbeitsplänen aber nicht der Grund für die Abwesenheit mitgeteilt werden. Für die Mitarbeiter macht es keinen Unterschied, ob der Kollege im Urlaub oder krank ist – entscheidend ist, dass er nicht da ist und für die Zeit seiner Abwesenheit evtl. Vertretungsregelungen zu beachten sind. Teilt der Arbeitgeber die Abwesenheitsgründe seiner Mitarbeiter der übrigen Belegschaft mit, sorgt er hierdurch möglicherweise nicht nur für Tratsch und Klatsch über den abwesenden Kollegen, sondern auch für eine unzulässige Übermittlung von Daten.

> **Praxistipp**:
>
> Bei betriebsöffentlichen Aushängen sollten Fehlzeiten der Beschäftigten ausschließlich in allgemeiner Form, beispielsweise als „abwesend“, aufgeführt werden.

Obwohl es eigentlich einen Grund zum Feiern gibt, liefern im Unternehmen geführte Geburtstagslisten immer wieder neuen Zündstoff für Konflikte. Den Zweck, zu sehen wie gut oder schlecht sich der ein oder andere Kollege hält oder zur „Pflege des Betriebsklimas“, mag eine Geburtstagliste vielleicht erfüllen. Zur Durchführung des Beschäftigungsverhältnisses ist sie aber nicht erforderlich.

Das Interesse des Einzelnen, für sich in Würde zu altern und Feierlichkeiten frei sozialer Zwänge nach eigener Entscheidung zu begehen, wiegt schwerer als das Interesse an sozialen Zwecken.

Praxistipp:

Möchte ein Unternehmen nicht auf eine Geburtstagsliste verzichten, empfehlen wir, jeden Mitarbeiter nach seiner Einwilligung zu bitten und ihn darüber zu informieren, dass er jederzeit aus der Liste gestrichen werden kann. Als Alternative kann den Mitarbeitern angeboten werden, auf die Angabe ihres Geburtsjahres zu verzichten.

3. Fall 11: Damit die Stimmung nicht kippt

Den meisten Arbeitgebern ist es ein Anliegen, dass ihre Mitarbeiter gerne zur Arbeit kommen. Motivation, Zufriedenheit und die nötige Wertschätzung steigern die Produktivität der Arbeit und damit auch den Umsatz des Unternehmens. Auf welchem Weg kann der Arbeitgeber das Stimmungsbild in seiner Firma aber am besten ausmachen? Hier wählen die meisten den Weg des vermeintlich geringsten Widerstands: die Mitarbeiterumfrage. Die Idee dahinter klingt verlockend: Der Mitarbeiter macht sich in Ruhe seine Gedanken zum vorgelegten Fragekatalog. Da er sicher ist, nicht als der Urheber des Bogens ausgemacht werden zu können, scheut er sich nicht, vorhandene Defizite anzusprechen. Dass Vorstellung und Realität nicht selten auseinanderfallen, zeigen wiederholt bei uns eingehende Beratungsanfragen zur Gestaltung von Mitarbeiterumfragen.

Im Rahmen eines internen Beurteilungssystems plante ein Betrieb, die Personen mit Führungsverantwortung durch alle Beschäftigten unter Verwendung eines Fragebogens beurteilen zu lassen. Auf die Anonymität der Umfrage wurde jedoch verzichtet, so dass uns ein Mitarbeiter des Unternehmens darum bat ihm mitzuteilen, ob er die Teilnahme an der Umfrage verweigern könne. Die Angst des Beschäftigten, bei einer Weigerung mit arbeitsrechtlichen Konsequenzen rechnen zu müssen, konnten wir ihm leider nicht nehmen. Auch wenn uns unsere Arbeit ohne tiefergehende arbeitsrechtliche Kenntnisse nicht möglich wäre, obliegt die Beantwortung solcher konkreten Fragen vorrangig den Arbeitsgerichten. Übrigens auch die Frage, ob sich Vorgesetze solche Umfragen gefallen lassen müssen. Das Abfragen subjektiver Einschätzungen über das Arbeitsumfeld, wie bspw. das Betriebsklima, ist gleichwohl nicht für die Durchführung des Beschäftigungsverhältnisses erforderlich und daher nur auf freiwilliger Basis möglich.

Praxistipp:

Wir empfehlen den verantwortlichen Stellen, die Mitarbeiterumfrage freiwillig und anonym durchzuführen und im Sinne der Transparenz die Beschäftigten über das Vorhaben und die angestrebten Ziele der Befragung rechtzeitig und umfassend zu informieren. Durch die Einschaltung eines Dienstleisters und des Abschlusses eines Vertrags zur Auftragsdatenverarbeitung kann die Anonymität der Umfrage gewährleistet werden. Nur so können Unternehmen ehrliche Antworten erwarten und Ergebnisse sinnvoll zur Verbesserung des Betriebsklimas. und die eigene Produktivität nutzen.

Auch wenn es keine festgeschriebene Antwort darauf gibt, ab welcher Aggregationsgröße – also dem Zusammenfassen von personenbezogenen Daten – kein Personenbezug mehr hergestellt werden kann, erscheint uns eine Mindestgröße von drei oder fünf allerdings als deutlich zu klein. Wir empfehlen eine Auswertung erst ab sieben Antworten vorzunehmen. In der medizinischen Forschung gehen wir inzwischen von Mindestgruppengrößen von 12 oder mehr aus.

4. Fall 12: „… and action“

Wählt man morgens für den Weg zur Arbeit die U-Bahn statt des Autos oder des Fahrrads, wurde man schon von der einen oder anderen optisch-elektronischen Einrichtung – einer Videokamera– erfasst. Kaum in der Firma angekommen, begegnet einem die nächste Kamera beim Betreten des Grundstücksgeländes. Verfolgt einen das Pech oder doch eher der Arbeitgeber selbst, hat dieser in sämtlichen Betriebsteilen Videokameras installiert. Selbstverständlich nur zu „Zwecken der Gefahrenabwehr und dem Schutz der eigenen Mitarbeiter“. Der Kreativität von Arbeitgebern, die Installation von Videokameras zu rechtfertigen, ist oft keine Grenze gesetzt.

Was aber ist der entscheidende Unterschied zwischen den Aufnahmen auf dem Weg zur Arbeit in der U-Bahn und der Kamera in den Betriebsräumen? In der U-Bahn geht es um die Überwachung von öffentlich zugänglichen Räumen, bei der Aufnahme in den Betriebsräumen um die Überwachung von Personen, nämlich Beschäftigter, im nicht-öffentlichen Bereich. Ein weiterer entscheidender Aspekt ist, dass der Beschäftigte morgens die Wahl zwischen U-Bahn und Videoaufnahme bzw. Auto und keiner Videoaufnahme hatte. Auch wenn dem Arbeitnehmer für Fälle unzulässiger

Videoüberwachung ein Unterlassungsanspruch zusteht und er seine Arbeitsleistung so lange aussetzen kann, bis der ihm zugewiesene Arbeitsplatz nicht mehr im Blickfeld der Kamera liegt[45], zeigen die täglich eingehenden Beschwerden, dass dieser Weg von den Beschäftigten meist nicht gewählt wird. Die Videoüberwachung stellt daher einen denkbar intensiven Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten dar.[46] Die Technik ermöglicht den Arbeitgebern, seine Beschäftigten in ihrer ganzen wahrnehmbaren Persönlichkeit zu beobachten (Monitoring) und reproduzierbar festzuhalten (Aufzeichnung).

Ob die Videoüberwachung zulässig ist, muss für jede Kamera gesondert geprüft werden und hängt von den Umständen des Einzelfalls ab: Welchen Zweck hat die Videoaufnahme? Ist von der Videoüberwachung die gesamte Belegschaft betroffen oder nur bestimmte Personen? Wie lange werden die Aufzeichnungen gespeichert? Sind die Betroffenen über den Einsatz von Videokameras ausreichend informiert oder findet eine heimliche Videoaufzeichnung statt? Hat der Arbeitgeber verbindlich zugesichert, die Aufzeichnungen nicht zum Nachteil der Beschäftigten einzusetzen?

Die Fälle, in denen Beschäftigte Opfer des Überwachungsdrangs ihres Arbeitgebers werden, stellen einen zunehmenden Bereich der täglichen Arbeit des LfDI BW dar.

Wie wir auch von Kollegen aus anderen deutschen Bundesländern erfahren haben, liegt es wohl im Trend vieler Bäckereiinhaber, die Verkaufstheke, also den ausschließlich für Mitarbeiter zugängliche Bereich, mit einer Videokamera zu versehen.

In einem Fall verdächtigte ein Bäcker einen seiner Verkaufsmitarbeiter, sich den einen oder anderen Euro in die eigene Tasche gesteckt zu haben. Da sich der Bäcker nicht mehr zu helfen wusste, installierte er in den Verkaufsräumen eine Videokamera, die ausschließlich den Thekenbereich umfasste. Nachdem sich der Verdacht gegen den einen Mitarbeiter bestätigte und die arbeitsrechtlichen Konsequenzen gezogen wurden, fand der Bäcker die Kamera so nützlich, dass er sie gleich hängen ließ. Da die Videoüberwachung den gesamten Thekenbereich und somit einen dauerhaften Arbeitsplatz der Mitarbeiter erfasste, lag ein massiver Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten vor. Je weniger Rückzugsmöglichkeiten dem Arbeitnehmer verbleiben, desto stärker wird er in seinem Recht auf informationelle Selbstbestimmung verletzt. Das ist illegal.

Der Gesetzgeber hat für Fälle, in denen bestimmte Mitarbeiter verdächtigt werden, während ihres Beschäftigungsverhältnisses Straftaten zu begehen, mit § 32 Abs. 1 Satz 2 BDSG eine klare Regelung getroffen, an der er durch § 26 Abs. 1 Satz 2 BDSG-neu auch über den 25. Mai 2018 hinaus festhält. Hiernach kann eine Videoüberwachung gegen einen konkreten Beschäftigten zulässig sein, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat. Diesen Zweck

[45] ArbG Dortmund 25.7.1988 – 6 Ca 1026/88 – CR 1989, 715.
[46] Vgl. BAG, Beschluss vom 29. Juni 2004 – 1 ABR 21/03 –, BAGE 111, 173-190.

hatte die installierte Videokamera im Fall des Bäckers aber bereits erfüllt. Die zeitlich darüber hinausgehende, rein präventive Videoüberwachung der anderen Mitarbeiter, war nicht mehr von § 32 BDSG (bzw. § 26 BDSG-neu) gedeckt und somit unzulässig. Die Videokamera wurde schließlich demontiert.

Auch in einem anderen Fall installierte ein Bäcker eine Videokamera, die ausschließlich den Thekenbereich erfasste. Der Zweck dieser Überwachung war aber weitaus origineller als beim vorgehenden Fall. Er bestand darin, den Thekenbestand zu überprüfen und die Bäckerei bei ausgehenden Broten und Kuchen entsprechend und zügig beliefern zu können. Auf unsere Nachfrage, ob nachzuliefernde Ware durch das Verkaufspersonal nicht einfach über das Telefon beim Bäcker angefragt werden kann, erhielten wir die dreiste Antwort, dass man dem Verkaufspersonal diese Fähigkeit nicht zutraue. Durch die Videoüberwachung nehme man diese vertrauensvolle Aufgabe lieber selbst in die Hand. Wie sich herausstellte, wurden die meisten Backwaren vor Ort durch das Verkaufspersonal aufgebacken und nicht, wie behauptet, ständig frisch angeliefert. Dem Bäcker sind die Argumente zur Rechtfertigung der Videokamera endgültig ausgegangen, sie wurde unverzüglich abgebaut. Er backt jetzt kleinere Brötchen …

III. Fall 13: Zum Abschied noch ein Datenschutzverstoß

Nicht immer endet ein Arbeitsverhältnis mit einem festen Handschlag und den besten Wünschen für den weiteren Lebensweg. Nicht selten werden die letzten Worte vor einem Arbeitsgericht gewechselt oder über die Rechtsbeistände ausgetauscht. Hält der ausgeschiedene Mitarbeiter dazu bereits ein anständiges Arbeitszeugnis in den Händen, scheut er sich nicht, der Aufsichtsbehörde alle scheinbaren Datenschutzverstöße der vergangen Jahre zu präsentieren. Arbeitsvertragliche Konsequenzen muss er bekanntermaßen nicht mehr befürchten und warum nicht den Kollegen zum Abschied was Gutes tun?

Bei allen Konstellationen steht der ehemalige Arbeitgeber vor der Frage: Was passiert mit den personenbezogenen Daten des ausgeschiedenen Mitarbeiters; wie und insbesondere wie lange müssen sie aufbewahrt werden? Dass Unternehmen die Antwort auf die Fragen hin und wieder erst nach der Trennung von einem Beschäftigten finden, zeigt unsere Beratungspraxis.

Bei einem Unternehmen sind in kürzester Zeit drei Beschäftigte ausgeschieden. Deren personalisierte E-Mail-Accounts wurden auch einige Zeit danach nicht von der Geschäftsführung gelöscht, sondern durchfilzt. Problematisch war, dass die Mitarbeiter ihre E-Mail-Accounts auch zu privaten Zwecken nutzten. Zwar fehlten Regelungen, die eine private Nutzung untersagten, aber eine etablierte betriebliche Übung hatte für Gegenteiliges gesorgt. Also war bereits die Einsichtnahme in die Accounts rechtswidrig. Das Unternehmen sah sich jedoch nicht in der Lage, die E-Mail-Accounts zu löschen, da die Geschäftsfortführung bedroht gewesen wäre. Sämtliche Kundenanfragen liefen bislang über die ausgeschiedenen Mitarbeiter.

Nicht mehr auf die E-Mail-Accounts zugreifen zu können hätte zum Auftragsverlust und angesichts der schwierigen wirtschaftlichen Lage des Unternehmens zur Insolvenz geführt.

Aufgrund unseres Einschreitens konnten die permanenten Verletzungen des Rechts auf informationelle Selbstbestimmung der ausgeschiedenen Mitarbeiter schnellstmöglich abgestellt werden. Der Zugriff auf die E-Mail-Accounts war ohne die Einwilligung der ehemaligen Beschäftigten nicht erlaubt. Durch unsere weitergehende Beratung hat das Unternehmen klare Regelungen für die Nutzung aller Informations- und Kommunikationstechniken schriftlich und verbindlich getroffen und seine Mitarbeitern entsprechend informiert.

Praxistipp:

Die meiste Geschäftskorrespondenz läuft heutzutage per E-Mail ab. Daher sollten Unternehmen es nicht versäumen, klare Löschkonzepte einzuführen. Nur so können die gesetzlichen Aufbewahrungspflichten, wenn die Korrespondenz als Handelsbrief einzustufen ist, eingehalten werden.

Ein durchgängiges Löschkonzept stellt durch organisatorische und technische Maßnahmen sicher, dass zum Ende des Verarbeitungszwecks die Löschung der Daten auch tatsächlich erfolgt.

Ob personenbezogene Daten nach dem Ausscheiden eines Mitarbeiters noch gespeichert werden dürfen bzw. müssen, hängt in erster Linie davon ab, ob spezielle Aufbewahrungsregelungen hierzu ermächtigen oder verpflichten.[47]

Wie lange Dokumente oder Akten aufzubewahren sind, bevor eine Löschung vorgenommen werden kann, ist abhängig von deren Inhalt. Für Unterlagen, die für die Besteuerung des Unternehmens relevant sind, geben die steuerrechtlichen Vorschriften eine Aufbewahrungszeit von sechs bzw. zehn Jahren vor. Darunter fallen beispielsweise die Buchungsbelege im Zusammenhang mit der Gehaltszahlung. Arbeitszeitnachweise sind zwei bzw. drei Jahre aufzubewahren, damit die Einhaltung von Arbeitszeitregelungen kontrolliert werden kann.[48]

Beide Seiten müssen jedoch für einen gewissen Zeitraum damit rechnen, dass aus dem beendeten Arbeitsverhältnis noch Rechte oder Pflichten geltend gemacht werden können, die nur schwer zu belegen sein werden, wenn die entscheidenden

[47] Gesetzliche Aufbewahrungsfristen finden sich bspw. in § 147 Abgabenordnung oder auch § 257 Handelsgesetzbuch.
[48] Vgl. § 16 Abs. 2 Arbeitszeitgesetz.

Unterlagen einen Monat nach der Beendigung vernichtet wurden.[49] Beispielsweise die Ausbezahlung von Urlaub und Überstunden an den Arbeitnehmer oder die Herausgabe eines dienstlichen Laptops an den Arbeitgeber. Nach § 195 des Bürgerlichen Gesetzbuches (BGB) verjähren solche Ansprüche grundsätzlich nach spätestens drei Jahren. Dabei beginnt gemäß § 199 BGB die Frist erst mit dem Ende des Jahres in dem der Anspruch entstanden ist.

C. Das Ziel unserer Arbeit

Wie die kleine Auswahl aus dem Bereich des Beschäftigtendatenschutzes gezeigt hat, ist die Arbeit des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg spannend und vielfältig. Auch wenn der Gesetzgeber uns vorrangig die Rolle einer Aufsichtsbehörde zugesprochen hat, richten wir unser besonderes Augenmerk auf die datenschutzrechtliche Beratung. Diese Rolle hat auch der europäische Gesetzgeber den Aufsichtsbehörden zugesprochen. Der Aufgabenkatalog aus Art. 57 Abs. 1 DSGVO ist lang und stellt auch die Behörden vor einige Herausforderungen. Mit diesem Ratgeber möchte der LfDI BW die Öffentlichkeit sowie die Verantwortlichen in Sachen Beschäftigtendatenschutz sensibilisieren und sie darüber aufklären.[50] Durch frühzeitige Einbindung unserer Behörde werden neue wirtschaftliche Entwicklungen im Betrieb nicht durch datenschutzrechtliche Anforderungen gehemmt, sondern langfristig und nachhaltig verbessert.

Der LfDI BW ist verpflichtet, neue Entwicklungen kritisch zu beobachten und zu begleiten. Ziel ist es nicht (nur) zu sagen, was alles nicht geht, sondern unter Berücksichtigung aller einzubeziehenden Interessen gemeinsam datenschutzkonforme Lösungen und Alternativen zu erarbeiten.

[49] Vgl. Art. 17 Abs. 3 lit. e) DSGVO.
[50] Vgl. Art. 57 Abs. 1 lit. b) und d) DSGVO.