Unsere Freiheiten:
Daten nützen - Daten schützen

Ratgeber Beschäftigtendatenschutz

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Der Landesbeauftragte für den Datenschutz
und die Informationsfreiheit Baden-Württemberg
Dr. Stefan Brink
Mitautor*innen: Johanna Krieger, Sabrina Schwab, Daniel Joos

Königstraße 10a
70173 Stuttgart

Telefon: (07 11) 61 55 41-0
Telefax: (07 11) 61 55 41-15

E-Mail: poststelle@lfdi.bwl.de
Homepage: https://www.baden-wuerttemberg.datenschutz.de/

Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende Geschlecht genannt. Selbstverständlich richtet sich dieser Bericht an die Angehörigen aller Geschlechter.

Stand: April 2020 (4. Auflage)

LfDI: Daten nützen – Daten schützen

Der Ratgeber

Arbeitnehmerdatenschutz: Zwischen wirtschaftlicher Abhängigkeit und informationeller Selbstbestimmung

Inhaltsverzeichnis

A. Einleitung

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 1.361 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]

Seit dem 25. Mai 2018 kommt die Datenschutz-Grundverordnung (DS-GVO) zur Anwendung. Auch sie lässt das Thema Beschäftigtendatenschutz trotz der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO nicht unberührt. Nach rund einem Jahr mit der DS-GVO haben wir genügend Grund, diesen Ratgeber auf den neusten Stand zu bringen!

B. 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[4] 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

[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 02/2019, www.iab.de.
[3] Dabei wird die Anonymität der Beschwerdeführer*innen gewahrt.
[4] BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83.

Datenschutzgesetzen vieler Länder.[5] Die Praxis musste solange auf die allgemeinen 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.

In Bezug auf den Regelungsbereich des Beschäftigtendatenschutzes fehlt es trotz entsprechender Bestrebungen des deutschen Gesetzgebers auch weiterhin an einem nationalen „Gesetz zur Regelung des Beschäftigtendatenschutzes“, das mit eigenständigen und spezifischen Regelungen die Besonderheiten des Arbeitsverhältnisses als Nähe- und Abhängigkeitsverhältnis beachtet. Dafür ist nun seit dem 25. Mai 2018 die EU-Datenschutz-Grundverordnung[6] mit ihrer unmittelbaren Bindung anzuwenden. Deren Ziel ist ein europaweites und einheitliches Datenschutzniveau. Für die Datenverarbeitung im Beschäftigungskontext hat der europäische Gesetzgeber in Art. 88 DS-GVO im Wege einer Öffnungsklausel ganz konkret die Möglichkeit für eigenständige nationale Regelungen geschaffen, die jedoch nicht zu einer absoluten Zersplitterung in diesem Bereich führen dürfen. In den Bereichen solcher Öffnungsklauseln ist nicht die DS-GVO anzuwenden, sondern das nationale Recht. Fehlen vorrangige datenschutzrechtliche Spezialgesetze, findet das BDSG als „Auffanggesetz“ Anwendung. Das Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung – BDSG – übernimmt zwar in seinem § 26 den bislang gültigen § 32 BDSG der alten Fassung mit wenigen Zusätzen, stellt aber nach wie vor nur einen Minimalkonsens dar. Einzige Neuerung in § 26 Abs. 1 BDS 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 –

[5] Vgl. bspw. § 36 Landesdatenschutzgesetz Baden-Württemberg.
[6] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

auch wenn noch ein paar Jahre ins Land ziehen werden, bis eine gefestigte Rechtsprechung zu erwarten ist.

I. Die Normenvielfalt im Beschäftigtendatenschutz

Auch die DS-GVO 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.[7]

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 …

Voraussetzung ist jedoch, dass die nationalen (Spezial-)Vorschriften im Einklang mit der DS-GVO 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 DS-GVO, sondern das nationale Recht anzuwenden. Beim Fehlen vorrangiger datenschutzrechtlicher Spezialgesetze findet das neue BDSG als „Auffanggesetz“ Anwendung[8], soweit es im Einklang mit dem höherrangigen EU-Recht steht. Im Unterschied zur bisherigen Subsidiaritätsregelung aus § 1 Abs. 3 BDSG a.F., sind die Anforderungen an spezialgesetzliche Regelungen jedoch gestiegen: andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften des BDSG nur vor, wenn sie einen Sachverhalt, für den das BDSG gilt, abschließend regeln. Andernfalls finden die Vorschriften des BDSG Anwendung. Aus diesem Grund ist eine Reihe von Gesetzesanpassungen nötig geworden, so beispielsweise auch in den

[7] Vgl. Art. 6 Abs. 1 DS-GVO.
[8] Vgl. § 1 Abs. 2 BDSG.

sozialrechtlichen Vorschriften. Rechtssicherheit wird man aber auch an dieser Stelle erst durch eine gefestigte Rechtsprechung erhalten.

Bereits die DS-GVO stellt in ihrem Art. 88 Abs. 1 klar, dass auch Kollektivvereinbarungen, wozu auch Betriebs- oder Dienstvereinbarungen zählen[9], 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 a.F. einzuordnen, ist künftig nicht mehr notwendig. Diese Klarstellung findet sich auch explizit in § 26 Abs. 4 BDSG. Der Hinweis auf Art. 88 Abs. 2 DS-GVO ist insoweit nur deklaratorisch. Machen die Mitgliedsstaaten oder die Kollektivparteien von Ihrer Möglichkeit aus Art. 88 Abs. 1 DS-GVO 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.[10] Wenn die DS-GVO von Grundrechten spricht, zählt hierzu neben dem uns bekannten, vom Bundesverfassungsgericht entwickelten Grundrecht auf informationelle Selbstbestimmung, das europäische Pendant, nämlich Art. 8 GR-Charta[11]. 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 Datenschutzbeauftragter 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.

DS-GVO-Tipp

Der neue europäische Handlungsrahmen zwingt zu einem Blick über den nationalen Tellerrand. Auch wenn die Rechtssetzung 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 DS-GVO als Chance begriffen werden. Der Schutz der eigenen Daten und damit der Persönlichkeit ist den betroffenen Personen gerade im

[9] Vgl. Erwägungsgrund 155 DS-GVO.
[10] Vgl. Art. 88 Abs. 2 DS-GVO.
[11] Charta der Grundrechte der Europäischen Union.

Beschäftigungsverhältnis ein hohes Anliegen. Unternehmen können sich durch ein gutes Datenschutzmanagement als erstrebenswerten Arbeitgeber verkaufen.

II. Die Regelungen der DS-GVO und des BDSG

1. Verarbeitung personenbezogener Daten

Die meisten in der DS-GVO verwendeten Begriffe ähneln den uns aus dem BDSG a.F. bekannten. Nach wie vor geht es beim Datenschutz um personenbezogene Daten. Was das bedeutet, erklärt nun Artikel 4 Nr. 1 DS-GVO: Personenbezogene Daten sind alle Informationen, 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".[12] 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. 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 (zusammengefassten Daten ohne Bezug zu einzelnen Personen) erreicht werden kann.

Seit der Anwendung der DS-GVO ist dies 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 DS-GVO im Gegensatz zum BDSG a.F. nicht zwischen dem Erheben, Verarbeiten oder Nutzen

[12] BAG, NZA 1995,185.

personenbezogener Daten. In Art. 4 Nr. 2 DS-GVO 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.

2. Anwendung auf alle Beschäftigten

Um nicht den Rahmen dieser Handreichung durch zahlreiche spezialgesetzliche Regelungen zu sprengen, wird hier nur auf § 26 BDSG und seine Voraussetzungen eingegangen. Diese Norm setzt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zum Zwecke eines Beschäftigungsverhältnisses voraus. Der Begriff des Beschäftigten wird nun in § 26 Abs. 8 BDSG 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 DS-GVO, insbesondere auf Art. 6 Abs. 1 S. 1 lit. f) DS-GVO, 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 im Vergleich zu § 32 BDSG a.F. länger ist, liegt daran, dass die Regelung besonderer Kategorien personenbezogener Daten direkt in § 26 BDSG selbst und nicht wie bislang in § 28 Abs. 6 bis 8 BDSG a.F. erfolgt. Diese Änderung ist aus Gründen der besseren Übersichtlichkeit zu begrüßen. Nach Art. 9 Abs. 1 DS-GVO 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 DS-GVO gegeben ist. Der deutsche Gesetzgeber hat für die besonders schutzbedürftigen Daten von der Öffnungsklausel aus Art. 9 Abs. 2 lit. b) DS-GVO Gebrauch gemacht und § 26 Abs. 3 BDSG 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.[13]

[13] Vgl. § 26 Abs. 4 BDSG.

***Praxistipp**:*

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

DS-GVO-Tipp:

Die DS-GVO 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 dem Recht auf Auskunft (Art. 15 DS-GVO) und Löschung (Art. 17 DS-GVO) – von der DS-GVO auch als „Recht auf Vergessenwerden" bezeichnet – noch weitergehende Rechte zu. Sie können nunmehr auch die Einschränkung der Verarbeitung (Art. 18 DS-GVO) sowie die Datenübertragung ihrer personenbezogenen Daten (Art. 20 DS-GVO) verlangen. Zur effektiven Rechtsausübung wurde in bestimmten Fällen die Möglichkeit eingeräumt, einer Verarbeitung personenbezogenen Daten zu widersprechen (Art. 21 DS-GVO).

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 hält der deutsche Gesetzgeber an der Vorschrift des alten § 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 DS-GVO umfasst ja ansonsten nur den Einsatz von Datenverarbeitungsanlagen bzw. setzt die geordnete Sammlung der Daten in Dateien voraus.[14] 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. 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,

[14] Art. 2 Abs. 1 DS-GVO.

wenn er einem Versuch unzulässiger Informationsbeschaffung ausgesetzt ist. Auch hier hilft ihm die datenschutzrechtliche Regelung.

5. Die Datenschutzgrundsätze

In Art. 5 Abs. 1 stellt die DS-GVO ihre Datenschutzgrundsätze vor. Die 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 DS-GVO 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.[15] Dass der Verantwortliche nach Art. 5 Abs. 2 DS-GVO zur Rechenschaft – Stichwort: Accountability – verpflichtet ist, kommt den Datenschutzaufsichtsbehörden ebenso wie den Betroffenen bei der Durchsetzung ihrer Rechte besonders zu Gute.

DS-GVO-Tipp:

Rechenschaft ablegen können Verantwortliche nur, wenn sie Daten-verarbeitungen in geeigneter Weise dokumentieren und die technischen und organisatorischen Maßnahmen entsprechend anpassen. Eine mögliche Form des Nachweises ist das Verarbeitungsverzeichnis nach Art. 30 DS-GVO. 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.

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

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 DS-GVO). Der Grundsatz umschreibt das bereits 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 DS-GVO als europäische Norm ausgelegt werden. Die englische Sprachfassung der DS-GVO

[15] Vgl. Art. 83 Abs. 5 lit. a) DS-GVO.

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 DS-GVO und die Rechte der Betroffenen in den Art. 15 ff. DS-GVO eine zentrale Rolle, wenn nicht sogar die Hauptrolle in der DS-GVO. Die Verarbeitung muss den Grundsatz der Transparenz wahren, also eine Verarbeitung personenbezogener Daten in einer für die betroffene Person nachvollziehbaren Weise.[16]

b. Zweckbindung (Art. 5 Abs. 1 lit. b) DS-GVO)

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 DS-GVO lockert den im BDSG strengen Zweckbindungsgrundsatz in gewisser Weise auf, indem sie in Art. 6 Abs. 4 DS-GVO 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 DS-GVO aber strenge Voraussetzungen vor, die erfüllt sein müssen.

c. Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO)

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung erforderliche Maß beschränkt sein. Hierunter versteht die DS-GVO den Grundsatz der Datenminimierung. Die Beschränkung auf das erforderliche Maß kennen wir aus dem BDSG als sogenannten Erforderlichkeitsgrundsatz. Der Grundsatz der Datenminimierung ist in den einschlägigen Rechtsnormen der DS-GVO enthalten (vgl. Art. 6 Abs. 1 S. 1 lit. b) bis f) und Art. 9 Abs. 2 lit. b), c), f) bis j) DS-GVO) und wird auch in § 26 BDSG 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

[16] Vgl. Erwägungsgrund 39 der DS-GVO.

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.[17] 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.[18] 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.

d. Richtigkeit (Art. 5 Abs. 1 lit. d) DS-GVO)

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.

DS-GVO-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 DS-GVO), sollte der vertretbare Aufwand nicht unterschätzt werden. Das zeigt insbesondere auch das Recht auf „Vergessenwerden“ aus Art. 17 Abs. 2 DS-GVO.

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

e. Speicherbegrenzung (Art. 5 Abs. 1 lit. e) DS-GVO)

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.

DS-GVO-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) DS-GVO).

f. Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DS-GVO)

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 DS-GVO.

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

III. Die Erfüllung der Informationspflichten gegenüber Beschäftigten

Dort, wo dem BDSG kein eigenständiger Regelungsgehalt zukommt bzw. dort, wo das BDSG die in der DS-GVO vorgesehen Öffnungsklauseln nicht nutzt, kommt es zur alleinigen Anwendung der DS-GVO bzw. einem Nebeneinander von europäischem und nationalem Recht. So auch im Bereich der Informationspflichten.

Ein Grund, warum die DS-GVO zur Mammutsaufgabe für die meisten Unternehmen wurde, sind die erhöhten Anforderungen an die Erfüllung der Informationspflichten, auch wenn diese nicht ganz neu sind: auch nach altem Recht musste der Verantwortliche die Betroffenen über die Verarbeitung ihrer Daten benachrichtigen (vgl. § 4 Abs. 3 und § 33 BDSG-alt). Vermutlich hat die Angst vor hohen Bußgeldern die Unternehmen dazu bewogen, ihre Informationspflichten seit der DS-GVO ernster zu nehmen. Im Vergleich zur alten Rechtslage ist der Umfang der Informationspflichten gestiegen. Welche Informationen die betroffene Person erhält,

bestimmt sich danach, ob der Verantwortliche die Daten beim Betroffen selbst (Art. 13 DS-GVO) oder einem Dritten (Art. 14 DS-GVO) erhoben hat. Denken Verantwortliche an die Erfüllung ihrer Informationspflichten, zeigt die Erfahrung des LfDI BW, dass Unternehmen erst nach und nach realisieren, dass die Informationspflichten nicht nur gegenüber den Kunden, sondern auch gegenüber den eigenen Beschäftigten bestehen. In den meisten Fallkonstellationen des Beschäftigtendatenschutzes richtet sich der Inhalt der Informationspflicht nach Art. 13 DS-GVO. Hiernach muss die betroffene Person, wie bislang auch, über die Identität des Verantwortlichen informiert werden (vgl. Art. 13 Abs. 1 lit. a) DS-GVO). Wer das ist, scheint im Bereich des Beschäftigtendatenschutzes ganz eindeutig zu sein. Ganz so leicht ist es insbesondere bei Konzernunternehmen oder bei Bereichen, die vom Verantwortlichen nicht im Wege der Auftragsverarbeitung, sondern dem altbekannten Begriff der Funktionsübertragung ausgelagert wurden, aber nicht immer. Auch die Beschäftigten müssen über die Kontaktdaten des Datenschutzbeauftragten informiert werden, sofern ein solcher bestellt wurde. Wie auch bisher muss über die Zwecke der Verarbeitung unterrichtet werden. Neu ist – und gerade 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) DS-GVO). Zwar gibt es im Bereich des Beschäftigtendatenschutzes wie eingangs erwähnt leider noch immer kein eigenständiges Beschäftigtendatenschutzgesetz und damit nur die allgemeine Vorschrift des § 26 BDSG, sodass man denken könnte, die richtige Rechtsgrundlage sei schnell gefunden. Die Fallstricke des Beschäftigten-datenschutzes zeigen aber, dass nicht selten das Gegenteil der Fall ist. Im Bereich des Beschäftigtendatenschutzes gibt es zahlreiche Spezialvorschriften. Beispielhaft ist § 39 Abs. 8 und 9 Einkommenssteuergesetz, der die Verarbeitung von auf der Lohnsteuerkarte enthaltenen Merkmalen regelt. Daneben können auch in Betriebsvereinbarungen eigeständige Erlaubnisnormen zur Verarbeitung personenbezogener Daten durch die Betriebsparteien geschaffen werden. Welche Rechtsgrundlage bei der Erfüllung der Informationspflichten anzugeben ist, kann somit sehr unterschiedlich ausfallen. Stützt der Verantwortliche die Verarbeitung von Beschäftigtendaten auf eigene, nach seiner Ansicht die Interessen oder Grundrechte und Grundfreiheiten des Beschäftigten überwiegende, Interessen, muss auch über diese informiert werden (Art. 13 Abs. 1 lit. f) DS-GVO). Im Gegensatz zum BDSG macht die DS-GVO keine Einschränkung über die Verpflichtung zur Mitteilung über die Empfänger oder Kategorien von Empfängern personenbezogener Daten, wenn bereits bei der Erhebung feststeht, dass diese personenbezogene Daten erhalten sollen (vgl. Art. 13 Abs. 1 lit. e) DS-GVO. Es kommt nicht mehr darauf an, ob der Betroffene nach den Umständen des Einzelfalls mit einer Übermittlung seiner Daten rechnen muss (vgl. § 4 Abs. 3 Satz 1 Nr. 3 BDSG-alt). Die DSGVO geht noch einen Schritt weiter und verpflichtet auch zur Mitteilung über eine Übermittlung personenbezogener Daten über den Geltungsbereich der DS-GVO hinaus (vgl. Art. 13 Abs. 1 lit. f) DS-GVO.

Wie aber erfüllen Arbeitgeber die weitreichenden Informationspflichten? Nach der Verordnung müssen die in Art. 13 oder Art. 14 DS-GVO aufgelisteten Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden. Im Bereich des Beschäftigten-datenschutzes empfiehlt der LfDI BW den Arbeitgebern, die Informationspflichten gegenüber den Mitarbeitern in einer Form vorzunehmen, die es den Beschäftigten jederzeit ermöglicht, die Information abzurufen. Hierfür können die im Unternehmen üblicherweise zur Verfügung stehenden Kanäle genutzt werden, wie zum Beispiel Veröffentlichungen im Intranet, ein zentraler Aushang am schwarzen Brett oder eine entsprechende E-Mail an alle Mitarbeiter. Es ist nicht notwendig, jedem Mitarbeiter ein persönliches Schreiben mit den nach der DS-GVO vorgesehen Informationen auszuhändigen und sich den Empfang des Schreibens bestätigen zu lassen. Ob der Mitarbeiter die ihm überlassenen Informationen zur Kenntnis nimmt, liegt ganz bei ihm. Keinesfalls sollten Unternehmen abstruse und – wie die tägliche Arbeit des LfDI BW zeigt – tatsächlich existierende Vorgehen wählen und dem Mitarbeiter bei Nichtbestätigung des Erhalts des Informationsschreibens mit der Kündigung drohen.

Praxistipp:

Verantwortliche dürfen nicht übersehen, dass die Informationspflichten auch gegenüber ihren eigenen Beschäftigten bestehen. Gerade in diesem Bereich bieten sich die im Unternehmen üblicherweise genutzten Kanäle zur Informationserteilung, wie das Intranet oder das schwarze Brett, an.

IV. 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 sind mit der DS-GVO noch weiter gestiegen: der Gestaltungsfreiraum von Arbeitgebern und Betriebsräten wird neben dem Schutzauftrag aus § 75 Abs. 2 BetrVG zusätzlich durch Art. 88 Abs. 2 DS-GVO 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 DS-GVO erlauben keine Absenkung des Datenschutzstandards gegenüber den Beschäftigten. Durch die in Art. 88 Abs. 2 DS-GVO 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 DS-GVO 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 heranzuziehen sind. All die Arbeit oft mühseliger Verhandlungen zwischen den Betriebsparteien hätte keinen Mehrwert gehabt. Hieran wird auch ein Arbeitgeber kein Interesse haben können.

DS-GVO-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 DS-GVO sind die Betriebsparteien gefragt. 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.[19] 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

[19] Vgl. Art. 57 Abs. 1 lit. d) DS-GVO.

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 Sensibilität für den Datenschutz zu schaffen.[20] Werden Prozesse von Anfang an unter dem Gesichtspunkt datenschutzrechtlicher Vorgaben vorangetrieben, werden Entwicklungen auch nicht ausgebremst, sondern von vornherein transparent und nachhaltig gestaltet. Unter dem neuen Datenschutzrecht nehmen die Aufsichtsbehörden noch mehr die Rolle des Beraters ein. 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 für den einzelnen betroffenen Beschäftigten ein positives Ergebnis 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[21] 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

[20] Vgl. Art. 57 Abs. 1 lit. d) DS-GVO.
[21] Vgl. § 88 Telekommunikationsgesetz.

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 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.[22] 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 (DSK) 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/datenschutzthemen 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.*

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

DS-GVO-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 DS-GVO nicht außer Acht gelassen werden dürfen. Arbeitgebern 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.

V. Einwilligung

Lässt sich die Verarbeitung personenbezogener Daten nicht auf eine gesetzliche Grundlage und insbesondere § 26 BDSG stützen, bleibt als weitere Datenverarbeitungsgrundlage die Einwilligung. Nach Art. 6 DS-GVO gilt das sogenannte Verbot mit Erlaubnisvorbehalt nach wie vor. Danach ist eine Verarbeitung personenbezogener Daten verboten, es sei denn, sie kann auf eine gesetzliche Ermächtigung oder eine wirksame Einwilligung gestützt werden. Unter „Einwilligung“ versteht die DS-GVO entsprechend ihrem Art. 4 Nr. 11 jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Wie sich aus Art. 6 Abs. 1 Satz 1 lit. a) DS-GVO ergibt, stellt die Einwilligung eine taugliche Rechtsgrundlage zur Verarbeitung von personenbezogenen Daten dar. In Umsetzung der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO erklärt § 26 Abs. 2 BDSG ausdrücklich, dass die Einwilligung auch im Beschäftigtenverhältnis möglich ist. Aufgrund der im Beschäftigungsverhältnis bestehenden Abhängigkeit der beschäftigten Person sind an die Einwilligung dort jedoch besondere Anforderungen zu stellen und die Umstände, unter denen die Einwilligung erteilt worden ist, speziell zu berücksichtigen. Während § 26 Abs. 2 S. 3 BDSG ausdrücklich die Schriftform für die Einwilligung fordert, fehlt eine solche Voraussetzung in der DS-GVO. Vielmehr ermöglichen Art. 7 Abs. 2 DS-GVO und der Erwägungsgrund 32, dass die Einwilligung schriftlich, elektronisch – etwa durch Setzen eines Häkchens (opt-in) oder auf einem digitalen Unterschriftenpad –, mündlich oder sogar konkludent erfolgen kann. Aus Beweisgründen ist es aber dennoch ratsam, die Einwilligung schriftlich zu fixieren. Damit die Einwilligung als Rechtsgrundlage herangezogen kann, muss die betroffene Person hinreichend bestimmt und transparent über die konkrete Tragweite ihrer Entscheidung aufgeklärt werden. Die einzelnen Verwendungszwecke sind deshalb ausdrücklich festzulegen und in Textform zu bezeichnen und aufzulisten. Schließlich ist ganz explizit auf die Freiwilligkeit der Erteilung der Einwilligung und die Sanktionslosigkeit bei ihrer Verweigerung hinzuweisen sowie auf die jederzeitige Möglichkeit des Widerrufs und dessen Folgen (Art. 7 Abs. 3 DS-GVO). Die aufsichtsrechtliche Praxis der Datenschutzbehörden

zeigt, dass es nicht selten an der notwendigen Freiwilligkeit der Einwilligung fehlt. Sie ist in der Praxis deshalb überwiegend in Konstellationen möglich, die nicht das Arbeitsverhältnis als solches, sondern nur Zusatzleistungen des Arbeitgebers betreffen (wie z.B. bei der Gestattung privater Nutzung der IuK oder dienstlicher Fahrzeuge, Telefone und EDV-Geräte, der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder der Aufnahme in Geburtstagslisten). Hingegen ist die Verarbeitung personenbezogener Daten von Beschäftigten häufig bereits zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich und kann deshalb auf § 26 BDSG als gesetzliche Grundlage gestützt werden, sodass es eines Rückgriffs auf eine Einwilligung gar nicht bedarf und davon sogar abzuraten ist. Andernfalls kann beim Arbeitnehmer der Eindruck entstehen, die Einwilligung werde vom Arbeitgeber als bloße „Pauschal-Lösung“ für alles herangezogen, ohne die gesetzlichen Anforderungen beachten zu wollen.

***Praxistipp**:*

Der LfDI BW rät aus den oben genannten Erwägungen grundsätzlich davon ab, für die Datenverarbeitung im Bereich des Beschäftigungsverhältnisses (zusätzlich) eine Einwilligung einzuholen. Soll dies dennoch geschehen, so ist zu empfehlen, in der Einwilligung explizit darauf hinzuweisen, dass die Datenverarbeitung darüber hinaus auch anhand der gesetzlichen Grundlage erfolgt. Aus denselben Gründen ist davon abzuraten, sich im Arbeitsvertrag eine Generaleinwilligung für die Datenverarbeitung des Beschäftigten geben zu lassen. Eine solche würde dem Transparenz- und Bestimmtheitsgebot nicht gerecht werden.

Fall 2: Die „freiwillige“ Urinprobe

Der minderjährige Beschwerdeführer befand sich in einem Berufsausbildungsverhältnis.[23] 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 DS-GVO) 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.

Art. 4 Nr. 11 der DS-GVO definiert, 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

[23] Zu den Beschäftigten im Sinne des BDSG zählen auch die zu ihrer Berufsausbildung Beschäftigten, vgl. § 26 Abs. 8 S. 1 Nr. 2 BDSG.

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 in Art. 7 DS-GVO. Besondere Bedingungen gelten für die Einwilligungen von Kindern in Bezug auf die Dienste der Informationsgesellschaft (vgl. Art. 8 DS-GVO).

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.[24]

Es reicht nicht aus, nur auf die Einwilligung zu verweisen. Vielmehr sind auch die Umstände, unter denen die Einwilligung abgegeben wird, einzubeziehen.[25] Eine Einwilligung beruht auf der freien Entscheidung des Betroffenen, wenn sie ohne Zwang abgegeben wird.[26] 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.[27]

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. In Art. 8 Abs. 1 DS-GVO wird eine Einwilligung für rechtmäßig erklärt, wenn das Kind das sechzehnte Lebensjahr erreicht hat. 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

[24] Vgl. vgl. Erwägungsgrund 42 Satz 4 der DS-GVO.
[25] Vgl. Art. 7 Abs. 4 DS-GVO.
[26] Vgl. Erwägungsgrund 42 der DS-GVO
[27] Dies belegt schon die Existenz des Berufsbildungsgesetzes.

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-alt 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.[28]

Die Erhebung besonderer Arten personenbezogener Daten war auch nicht nach § 28 Abs. 6 Nr. 3 BDSG-alt erlaubt und wäre es auch nicht nach dem heutigen § 26 Abs. 3 BDSG 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.*

[28] Vgl. § 26 Abs. 3 Satz 2, letzter Halbsatz BDSG.

DS-GVO-Tipp:

Auch wenn der Streit, ob eine Einwilligung auch im Beschäftigungsverhältnis möglich ist, durch Art. 6 Abs. 1 lit. a) DS-GVO und § 26 Abs. 2 BDSG 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 DS-GVO, muss nach § 26 Abs. 2 BDSG 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 DS-GVO vorausgesetzt, muss die Einwilligung schriftlich erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (vgl. § 26 Abs. 2 DS-GVO). Ob der nationale Gesetzgeber mit dem Schriftformerfordernis in unzulässiger Weise über die Anforderungen der DS-GVO hinausgeht und damit unwirksam ist, wird sich zeigen, Aus Beweisgründen ist eine schriftliche Einholung der Einwilligung aber jedenfalls ratsam.

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.[29] Gleichzeitig werden Inhalte und Grenzen dieses Fragerechts durch das „Recht zur Lüge“[30] bei unzulässigen Fragen konterkariert und können auch mithilfe einer Einwilligung nicht erweitert werden. § 26 BDSG 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.

[29] Vgl. auch BAG 22.10.1986 – 5 AZR 660/85 – DB 1987, 1048.
[30] BAG AP Nr. 2 zu § 123 BGB, st. Rspr.

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.[31] Allerdings besteht die Möglichkeit für den Arbeitgeber, 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.

[31] Thüsing, Arbeitnehmerdatenschutz und Compliance, Rn. 387.

- 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.

> ***DS-GVO-Tipp:***
>
> *Wie Art. 10 DS-GVO zeigt, bleibt das Verlangen von Arbeitgebern nach Auskunft und die Nutzung personenbezogener Daten über Vorstrafen wie gewohnt schwierig. Es besteht nach wie vor 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 – 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.

DS-GVO-Tipp:

Nach dem Willen des europäischen Verordnungsgebers ist die Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO, wozu auch die Gesundheitsdaten von Beschäftigten gehören, grundsätzlich verboten, wenn nicht eine der Ausnahmen nach Art. 9 Abs. 2 DS-GVO greift. Von der Öffnungsklausel aus Art. 9 Abs. 2 lit. b) DS-GVO hat der deutsche Gesetzgeber durch § 26 Abs. 3 BDSG 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), 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 ein Entwurf blieben, findet sich der Aussagegehalt der vorstehenden Regelung im heutigen § 26 BDSG wieder. In der DS-GVO ist nicht normiert, dass personenbezogenen Daten grundsätzlich beim Betroffenen zu erheben sind. Auch wenn der Direkterhebungsgrundsatz nicht unmittelbar aus der DS-GVO abgelesen werden kann, ergibt er sich doch zumindest mittelbar: Art. 5 DS-GVO sowie 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 – wie oben bereits erörtert – jedenfalls erheblich erweitert.

> ***DS-GVO-Tipp:***
>
> *Auch wenn der Direkterhebungsgrundsatz nicht ausdrücklich in der DS-GVO normiert ist, ergibt er sich jedoch mittelbar aus ihr und dem Grundrecht auf Datenschutz. Arbeitgeber sollten 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 DS-GVO 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 von Art. 7 Abs. 4 i.V.m. § 26 Abs. 2 BDSG geforderte Freiwilligkeit verneinen zu müssen.

***Praxistipp**:*

Pre-Employment-Screenings (PES) auf klarer gesetzlicher Grundlage sind zulässig, wenn sie datenschutzkonform durchgeführt werden. Dies bedeutet auch, dass der Arbeitgeber bei jedem Screening seine Informationspflichten gemäß Art. 14 DS-GVO auslöst und den Betroffenen in fairer und transparenter Weise seine „Treffer" offenlegen muss.

Wir empfehlen dringend, auf die Durchführung von PES zu verzichten, wenn diese nicht datenschutzkonform (ohne Rechtsgrundlage) durchgeführt werden können. Denn Arbeitgebern stehen genügend andere 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 DS-GVO ist dies allemal. Im öffentlichen Bereich gibt es mit § 15 Abs. 3 Landesdatenschutzgesetz (LDSG) für diesen Aspekt sogar eine konkrete Regelung, die den Kontakt zum ehemaligen Dienstherrn ohne Einwilligung untersagt.

DS-GVO-Tipp:

Denken Arbeitgeber weiterhin, dass sie mit ehemaligen Arbeitgebern eine Art arbeitsrechtliche Schicksalsgemeinschaft bilden würden, die sie zur Nachfrage bei diesem berechtigten würden (wovon die DS-GVO allerdings nichts weiß), wäre der alte Arbeitgeber zur Informationsmitteilung auch 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-Diskriminierungs-prozesses 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.[32] 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. Hinzu kommt, dass auch bei Einreichung einer solchen Klage beim Arbeitsgericht zunächst noch die Zustellung der Klage an den Beklagten erfolgen muss, was wiederum Zeit in Anspruch nimmt. Dafür muss deshalb ebenfalls ein zeitlicher „Puffer“ eingerechnet werden. Angelehnt an eine diesbezüglich eingeholte Auskunft bei den Arbeitsgerichten des Landes Baden-Württemberg geht der LfDI BW von einem Zeitraum von etwa 10 Werktagen aus, der im Durchschnitt

[32] Vgl. § 1 Allgemeines Gleichbehandlungsgesetz.

bis zur Klagezustellung durch das Gericht verstreicht. Unter Berücksichtigung aller möglicherweise eintretenden Verzögerungen bei der Zustellung weitet er den Zeitraum deshalb aus Kulanz auf zusätzliche zwei Monate aus. Der LfDI BW hält eine Speicherung von Bewerbungsunterlagen nach Abschluss des Auswahlverfahrens über vier Monate hinaus daher für nicht erforderlich und empfiehlt Arbeitgebern, nach Ablauf dieser Zeitspanne eine (automatische) Löschung zu veranlassen.

> ***Praxistipp**:*
>
> *Um die Löschfrist von vier 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 aufgrund dieser Einwilligung 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 informieren, wie seine personenbezogenen Daten verarbeitet werden. Hierzu gehört auch eine Mitteilung, wie die Daten übertragen werden – hoffentlich auch verschlüsselt!.

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 und nur Kontaktaufnahmen, die mit der Eingehung eines Beschäftigungsverhältnisses im konkreten Zusammenhang stehen, zu einer Verlängerung der Speicherdauer um sechs Monate führen.

Praxistipp:

Entscheidet sich ein Unternehmen, Bewerbungsportale zu nutzen und den Bewerbern mit ihrer Einwilligung 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.

DS-GVO-Tipp:

Die Anforderungen an die Datenschutzhinweise sind durch die DS-GVO 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 DS-GVO sogar noch weiter ausgeweitet: Die DS-GVO stärkt die Transparenz der Verarbeitung weiter, indem sie es 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) DS-GVO).

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 Aufsichtsbehörde 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 darauf 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.[33] Da das Jobcenter beim 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.

DS-GVO-Tipp:

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

[33] Vgl. § 57 SGB II.

6. Fall 8: Künstliche Intelligenz im HR-Bereich

Künstliche Intelligenz hält zunehmend auch im HR-Bereich Einzug. Zum einen greifen viele Personalabteilungen zu sog. „Chat Bots“ zurück, welche die Kommunikation mit (potentiellen) Bewerber*innen oder die Bearbeitung von Anfragen zum Bewerbungsprozess 24/7 und unabhängig von Abwesenheiten der Recruiter übernehmen können. Die Möglichkeiten von Künstlicher Intelligenz wecken aber auch andere Begehrlichkeiten. Insbesondere soll durch den Einsatz von automatisierten Verfahren der Auswahlprozess effektiviert und charakterlich „passende“ neue Mitarbeiter*innen gefunden werden. Die KI nimmt hier in der Regel eine Vorauswahl der Bewerber*innen anhand bestimmter persönlicher Gesichtspunkte vor. Die DS-GVO setzt hierbei die Rahmenbedingungen und Arbeitgeber haben bei der Nutzung von KI auf den datenschutzkonformen Einsatz zu achten und die Rechte der Betroffenen zu berücksichtigen. Die besondere Relevanz für den Datenschutz zeigt folgender Beispielsfall:

Ein Unternehmen lässt im Rahmen des Auswahlverfahrens den Text des Motivationsschreibens der Bewerbung sowie die Sprache der Kandidat*innen durch ein automatisiertes Verfahren analysieren, um bestimmte Eigenschaften der Persönlichkeit und des Charakters zu beurteilen. Die KI erstellt hierbei ein Ranking der Kandidat*innen, welche von den Recruiter, ohne nähere Prüfung, zur Grundlage für die Entscheidung zur Einladung zum Bewerbungsgespräch oder sogar für die Einstellung selbst gemacht wird.

Dabei handelt es sich zunächst um eine (automatisierte) Verarbeitung von personenbezogenen Daten gem. Art. 2 Abs. 1, Art. 4 Nr. 1 DS-GVO. Diese Vorgehensweise ist datenschutzrechtlich in zweierlei Hinsicht relevant. Zum einen liegt in der automatisierten Text-/ Sprachanalyse ein sog. Profiling i.S.d. Art. 22 DS-GVO. Zum anderen handelt es sich um eine Datenverarbeitung im Beschäftigtenkontext, welche einen Erlaubnistatbestand nach der DS-GVO bzw. dem BDSG voraussetzt. Ein Rückgriff auf eine Einwilligung wird im Kontext der Bewerbung und mit Blick auf die notwendige Freiwilligkeit nur in seltenen Fällen möglich sein. Dies hat zur Folge, dass die konkrete Analysetiefe der Sprache bzw. des Motivationsschreibens der Kandidat*innenen, vollumfänglich „erforderlich“ i.S.d § 26 Abs. 1 S. 1 BDSG für die Begründung des Beschäftigungsverhältnisses sein muss. Dies muss durch die verantwortliche Stelle nachvollziehbar und überzeugend dargelegt werden.

Ferner müssen Vorkehrungen getroffen werden, dass unrichtig generierte personenbezogene Daten korrigiert werden können, die Betroffenen spezifisch über das Ergebnis unterrichtet werden bzw. bei Bedarf die Kandidat*innen ihren abweichenden Standpunkt darlegen können (vgl. S. 4, Erwägungsgrund 71 zur DS-GVO). Auch steht den Kandidat*innen gem. Art. 22 Abs. 1 DS-GVO das Recht zu, „*nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden*“. Die KI kann somit nur eine Entscheidungshilfe darstellen, mit Vorbehalt der endgültigen Entscheidung durch einen menschlichen Recruiter. Das Kandidatenranking der KI muss somit vor jeder Entscheidung und in jedem Einzelfall „menschlich“ überprüft werden.

Im juristischen Schrifttum werden zu KI basierter Bewerberauswahl bislang unterschiedliche Ansichten vertreten -- aus Sicht einer Aufsichtsbehörde ist die Vorgehensweise nicht unkritisch. Vor diesem Hintergrund ist insbesondere zu bedenken, dass die erhobenen Informationen über potentielle Mitarbeiter*innen durch das seitens der Rechtsprechung entwickelte „Fragerecht des Arbeitgebers“ abgedeckt sind, begrenzt durch das „Recht zur Lüge“ bei unzulässigen Fragen.[34] Durch KI basierte Bewerberanalyse dürfen somit keine an sich für das Beschäftigungsverhältnis nicht „erforderlichen“ Daten zur Persönlichkeit der Kandidat*innen„durch die Hintertür“ verarbeitet werden.

***Praxistipp**:*

*Die Anwendungsmöglichkeiten von KI im Rahmen der Personalarbeit sind vielseitig. Wenn es zum Einsatz von KI von Seiten der verantwortlichen Stelle kommt, ist Transparenz und Kennzeichnung für die Betroffenen unverzichtbar. Auch bei dem Einsatz von „Chat Bots“ sollte den Bewerber*innen stets klar gemacht werden, dass nicht mit einem Mensch, sondern einem automatisierten Assistenzsystem kommuniziert wird.*

DS-GVO-Tipp:

Entscheidet sich eine verantwortliche Stelle zu KI basierter Bewerberanalyse ist zu beachten, dass diese selbst (und nicht der Hersteller von entsprechenden Programmen) verantwortlich für die Einhaltung der Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO ist und deren Einhaltung auch vollumfänglich nachweisen können muss. Dazu gehört, dass der Verantwortliche vollumfänglich den Informations-/ und Auskunftspflichten nach der DS-GVO unterliegt. Dies betrifft insbesondere die Frage, „nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann“ (vgl. S. 3, Erwägungsgrund 63 zur DS-GVO), auch wenn das eingesetzte KI-Produkt von einem (anderen) Hersteller entwickelt wurde. Mit Blick auf Art. 22 Abs. 1 DS-

[34] Vgl. hierzu auch Fall 4, S. 28 ff.

GVO ist es zudem unerlässlich, dass die finale Entscheidung hinsichtlich des Kandidaten, durch den Recruiter getroffen wird.

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-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 DS-GVO 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 DS-GVO). 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. DS-GVO erfüllt werden. Entsprechend den Informationspflichten der DS-GVO 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 Betriebs-vereinbarungen 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.

DS-GVO-Tipp:

Das Prinzip von Datenschutz durch Technikgestaltung (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) findet sich auch in Art. 25 DS-GVO. 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 DS-GVO im Gegensatz zum alten BDSG nicht zwischen dem Erheben, Verarbeiten oder Nutzen personenbezogener Daten. In Art. 4 Nr. 2 DS-GVO werden verschiedenen Verwendungsarten personenbezogener Daten unter den einheitlichen Begriff der Verarbeitung gefasst. Die in Art. 4 Nr. 2 DS-GVO aufgelisteten, nicht abschließenden Beispiele zeigen, dass die DS-GVO von einem weiten Begriffsverständnis ausgeht und „jeden Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ mit einbezieht.

a. Das Mutter-Tochter-Verhältnis

Innerhalb einer Unternehmensgruppe oder eines Konzerns ist die Weitergabe von Beschäftigtendaten häufig besonders bedeutend, da die zunehmende Verflechtung von Unternehmensstrukturen zu einer Verschiebung von Weisungs- und Kontrollbefugnissen auf Seiten des Arbeitgebers führen kann. Ohne Zugriff auf die personenbezogenen Daten der Mitarbeiter können diese Befugnisse unter Umständen nicht adäquat ausgeführt werden. Denkbare Anwendungsbereiche sind zahlreich, so zum Beispiel die Aufnahme von Mitarbeiterdaten in zentrale Programme der Personalverwaltung, die Inanspruchnahme eines gemeinsamen Rechenzentrums oder die konzernweite Einrichtung eines Telefonverzeichnisses. Da es an spezialgesetzlichen Normen fehlt, muss auf die DS-GVO bzw. das BDSG zurückgegriffen werden. Ein sogenanntes „Konzernprivileg“, also rechtliche Erleichterungen bzw. Privilegierungen aufgrund der einheitlichen wirtschaftlichen Tätigkeit, ist sowohl der DS-GVO als auch dem BDSG – nach wie vor – fremd. Jedes eigenständige Unternehmen, das Teil dieser Unternehmensgruppe oder des

Konzerns ist, stellt grundsätzlich also jeweils eine eigene verantwortliche Stelle dar. Jeder Austausch von Daten bedarf einer Rechtsgrundlage. Weist das Arbeitsverhältnis als solches einen Konzernbezug auf, der schon bei Beschäftigungsbeginn im Arbeitsvertrag festgehalten wurde, weil der Beschäftigte beispielsweise nicht mehr nur „einen“ Arbeitgeber hat und/oder an andere Konzerngesellschaften entsendet werden kann, liegt es auf der Hand, dass der Austausch von Daten innerhalb der Konzernstruktur für den Arbeitgeber für die Durchführung des Beschäftigungsverhältnisses im Sinne des § 26 BDSG erforderlich ist. Werden die personenbezogenen Daten zum Beispiel durch eine zentrale Personalabteilung verwaltet, der gegenüber ein Weisungsrecht besteht, kann die Verarbeitung durch eine Auftragsdatenverarbeitung erfolgen. Liegt der konkrete Konzernbezug nicht schon von sich aus vor und ist die Übermittlung deshalb nicht bereits für die Zwecke des Beschäftigungsverhältnisses erforderlich, können Unternehmen auch berechtigte Interessen nach Art. 6 Abs. 1 S. 1 lit. f) DS-GVO geltend machen. Wie Erwägungsgrund 48 der DS-GVO zeigt, können Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen und dabei einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse daran haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Der europäische Gesetzgeber betrachtet Konzernunternehmen in der Regel also als gemeinsame Verantwortliche (Art. 26 DS-GVO), wobei vertraglich insbesondere eine Festlegung darüber erfolgen muss, welches Unternehmen für die Erfüllung welcher Betroffenenrechte zuständig ist. Jede Datenübermittlung erfordert dabei eine Einzelfall-Abwägung der Interessen des Verantwortlichen und des betroffenen Beschäftigten und muss sowohl fair, transparent, verhältnismäßig und zweckgebunden als auch auf das erforderliche Maß beschränkt sein. Die Aufnahme in einen Talentpool hingegen ist nur mit Einwilligung des Bewerbers möglich. Im Rahmen der Einwilligung muss der Bewerber darüber informiert werden, dass alle konzernangehörigen Unternehmen auf seine personenbezogenen Daten zugreifen können.

Praxistipp:

Für die praktische Umsetzung der datenschutzrechtlichen Anforderungen kommen insbesondere speziell ausgearbeitete (Konzern-)Betriebs-vereinbarungen als Grundlage für die konzerninterne Datenweitergabe in Betracht, durch die eine gesteigerte Rechtssicherheit erreicht werden kann. Solche Vereinbarungen müssen den strengen Voraussetzungen des Art. 88 Abs. 2 DS-GVO entsprechen.

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

c. Fall 10: Der Mitarbeiter als Aushängeschild

Es stellt sich immer wieder die Frage, wie mit Mitarbeiterfotos zu verfahren ist, wenn das Arbeitsverhältnis beendet worden ist.

In der Anfrage eines Unternehmens ging es um ein Gruppenfoto der Belegschaft, auf welchem auch ein ehemaliger Arbeitnehmer unter ca. einem Dutzend anderer Kollegen abgebildet war. Über diese im Netz veröffentlichte Nutzung hatte sich nun der ehemalige Arbeitnehmer beschwert. Er verlangte, dass sein Foto herunter genommen wird. Statt einer Löschung wurde nun aber auf dem Foto sein Kopf heraus- und der eines anderen Person per Foto-Retusche hereingeschnitten. Geht das?

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.[35] Damit die Einwilligung wirksam ist,

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

muss sie zwingend vor – und nicht erst nach – der Aufnahme und ihrer Veröffentlichung eingeholt werden. Weiterhin sind die strengen Voraussetzungen für eine Einwilligungserklärung zur Informiertheit, Bestimmtheit und Transparenz zu beachten. Werden diese erfüllt, spricht bezüglich der Verarbeitung von Mitarbeiter-Fotos auch nichts dagegen, die Einwilligung in Form einer Generalerklärung einzuholen, die sich allgemein auf sämtliche Fotoaufnahmen bei internen Veranstaltungen und die entsprechenden Zwecke der Verarbeitung bezieht. Lediglich, wenn sich der beabsichtigte Zweck der Verarbeitung der Fotografie nachträglich ändert, ist erneut eine separate Einwilligungserklärung notwendig. Vom ursprünglichen Vorliegen der erforderlichen Einwilligung konnten wir im vorliegenden Fall ausgehen. Diese wurde vom ehemaligen Beschäftigten widerrufen. Ein Widerruf verpflichtet das Unternehmen zur Löschung. Andererseits führt das Ende des Arbeitsverhältnisses nicht automatisch zum Erlöschen des Rechts des Arbeitgebers an der Verwendung von Mitarbeiterfotos. Es darf nicht übersehen werden, dass es – auch finanziell – sehr aufwändig wäre, wenn der Arbeitgeber jedes Mal, wenn jemand aus dem Unternehmen ausscheidet, sämtliche Belegschaftsfotos erneuern oder die Person unkenntlich machen müsste. Da es sich bei den Bildern auf der Internetseite nicht um die Aufnahmen einzelner Personen handelte, denen eine Identität klar zugeordnet werden konnte, sondern um solche von größeren Gruppen, durch die jeweils alle Mitarbeiter gezeigt wurden, kamen wir zu dem Ergebnis, dass es dem Unternehmen bei der Verwendung der Bilder augenscheinlich um eine allgemeine Darstellung des Unternehmens ging. Einzelne Personen und Persönlichkeiten der Arbeitnehmer wurden nicht hervorgehoben, ihre Namen nicht genannt und die Identität ihrer Person auch sonst nicht herausgestellt. Zudem entstand beim Betrachter nicht zwingend der Eindruck, es handele sich zweifelsohne um die vollständige aktuelle Belegschaft. Durch die Demontage des Kopfes des Betroffenen und das Einsetzen des Kopfes einer anderen Person auf den Fotos konnte der Anspruch des Betroffenen, nicht mehr hinreichend erkennbar bzw. identifizierbar zu sein, deshalb ausreichend erfüllt werden, sodass kein Recht auf vollumfängliche Löschung bestand.

***Praxistipp**:*

Widerruft der Beschäftigte seine Einwilligung, bleibt dem Arbeitgeber mangels anderer Rechtsgrundlage, auf die er die Verarbeitung stützen könnte, keine andere Wahl: Das Foto muss weg oder zumindest retuschiert werden, um eine Identifizierung auszuschließen.

DS-GVO-Tipp:

Die Entscheidung des BAG kann unter Geltung der DS-GVO 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 DS-GVO übertragen werden. Zwar bleibt dem nationalen Gesetzgeber gemäß Art. 85 Abs. 2 DS-GVO 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 DS-GVO keinen eigenen Regelungsspielraum vor. Die Rechtsprechung des BAG widerspricht Art. 7 Abs. 3 DS-GVO, der einen jederzeitigen Widerruf der Einwilligung voraussetzt. Der Arbeitgeber hat gemäß § 26 Abs. 2 Satz 4 BDSG die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Abs. 3 DS-GVO 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 Abs. 1 lit. b) DS-GVO).

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 auch 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. Außerdem 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 Fragenkatalog. 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 selbst 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 den Abschluss 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 Personen 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 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 Beschäftigten, im nicht-öffentlichen Bereich. Ein weiterer entscheidender Aspekt ist, dass der Beschäftigte morgens die Wahl zwischen U-Bahn mit Videoaufnahme bzw. Auto ohne 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[36], zeigen die täglich eingehenden Beschwerden, dass dieser Weg von den Beschäftigten meist nicht gewählt wird. Die Videoüberwachung stellt einen denkbar intensiven Eingriff in das informationelle Selbstbestimmungsrecht

[36] ArbG Dortmund 25.7.1988 – 6 Ca 1026/88 – CR 1989, 715.

der Beschäftigten dar.[37] Die Technik ermöglicht es den Arbeitgebern, ihre 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?

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 zugänglichen 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 den 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 diesem Recht verletzt. Das ist illegal.

Der Gesetzgeber hat für Fälle, in denen bestimmte Mitarbeiter verdächtigt werden, während ihres Beschäftigungsverhältnisses Straftaten zu begehen, mit § 26 Abs. 1 Satz 2 BDSG eine klare Regelung getroffen. 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 hatte die installierte Videokamera im Fall des Bäckers aber bereits erfüllt. Die darüber hinausgehende, rein präventive Videoüberwachung der anderen Mitarbeiter ist nicht mehr von § 26 BDSG 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 vorhergehenden 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

[37] Vgl. BAG, Beschluss vom 29. Juni 2004 – 1 ABR 21/03 –, BAGE 111, 173-190.

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 …

5. Fall 13: Personalleasing – Datenverarbeitung im Auftrag?

Neben klassischen Beschäftigungsverhältnissen entspricht es der betrieblichen Realität, dass auch Fremdpersonal zum Einsatz kommt. Neben den arbeitsrechtlichen Besonderheiten des Arbeitnehmerüberlassungsgesetzes wirft dies auch datenschutzrechtlich etliche Fragen im Verhältnis zwischen Verleiher und Entleiher auf, wie folgender Praxisfall zeigt:

Die Leiharbeitnehmer*innen eines Personaldienstleisters sind im Wege der Arbeitnehmerüberlassung im Betrieb des Entleihers eingesetzt. Vor diesem Hintergrund sind die Leiharbeitnehmer*innen des Verleihers naturgemäß, wie eigene Beschäftigte des Entleihers, in den Betrieb des Entleihers eingegliedert. Dies bedeutet auch, dass sie bei den Repräsentanten bzw. Vorgesetzten, entsprechend der vereinbarten Berichtslinie, Arbeitsanweisungen entgegen nehmen, sich bei den Zugangskontrollen an-/ und abmelden und vor Ort ihre Pausen in das System zur Arbeitszeiterfassung eintragen. Demnach verarbeiten bei der Arbeitnehmerüberlassung sowohl der Verleiher als auch der Entleiher personenbezogene Daten der Leiharbeitnehmer*innen. Im Zuge des Vollzugs der Arbeitnehmerüberlassungsvertrages übersenden Entleiher den Verleihern daher oftmals eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO mit der Begründung, dadurch den datenschutzrechtliche Anforderungen nachzukommen. Diese Argumentation verkennt allerdings die datenschutzkonforme Ausgestaltung des Leiharbeitsverhältnisses.

Gem. § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten nur für Zwecke des Beschäftigungsverhältnisses, etwa zur Durchführung, verarbeitet werden. Aus § 26 Abs. 8 Nr. 1 BDSG ergibt sich ergänzend, dass Beschäftigte im Sinne dieses Gesetzes „*Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher*“ sind. Dies soll klarstellen, „*dass Leiharbeitnehmer nicht nur im Verhältnis zum Verleiher, sondern auch im Verhältnis zum Entleiher als Beschäftigte gelten*“[38] und dieser sie hinsichtlich des datenschutzrechtlichen (Schutz-) Status, wie eigene Arbeitnehmer*innen behandeln muss. Dies führt allerdings auch zu dem Ergebnis, dass eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO zwischen Verleiher und Entleiher nicht in Frage kommt. Der Verleiher verarbeitet keine personenbezogenen Daten auf Weisung, unter Kontrolle oder für Zwecke des Entleihers, wie es Art. 28 DS-GVO voraussetzen würde.[39] In der betrieblichen Realität verarbeiten der Entleiher und Verleiher die personenbezogenen Daten entweder für gemeinsame Zwecke oder jeweils für eigene Zwecke im Rahmen der Durchführung ihres Arbeitnehmerüberlassungsvertrages, also beispielsweise von der einen Vertragsseite zur Rechnungsstellung oder Überprüfung des (Fremd-) Personaleinsatzes und von der anderen Seite zur Personalorganisation.

[38] BT-Drucks 18/11325, S. 99
[39] DSK Kurzpapier Nr. 13 zur Auftragsverarbeitung, Art. 28 DS-GVO, Stand: 17.12.2018

Dies führt zur Folgefrage, wie die Verantwortlichkeit des Verleihers und Entleihers mit Blick auf Art. 4 Nr. 7 DS-GVO zu qualifizieren ist. In Frage kommt sowohl eine je eigene Verantwortlichkeit, als auch eine gemeinsame Verantwortlichkeit gem. Art. 26 DS-GVO[40]. Für eine eigene Verantwortlichkeit lässt sich zunächst anführen, dass Verleiher und Entleiher jeweils primär zu eigenen Zwecken Daten verarbeiten und mit Blick auf § 26 BDSG, jede Datenverarbeitung im Beschäftigtenkontext vom Erlaubnistatbestand umfasst sein muss.

***Praxistipp**:*

*Im Bereich der Arbeitnehmerüberlassung ist für die betroffenen Leiharbeitnehmer*innen entscheidend, dass transparent dargestellt werden kann, von welcher Vertragsseite welche personenbezogenen Daten erhoben und verarbeitet werden. Diese Transparenz ist vor dem Hintergrund der vielen Datenübermittlungen zwischen Verleiher und Entleiher unerlässlich, weshalb die Betroffenenrechte der DS-GVO gegenüber beiden geltend gemacht werden können.*

DS-GVO-Tipp:

*Die DS-GVO fordert sowohl vom Verleiher als auch dem Entleiher neben der Einhaltung der Betroffenenrechte und Durchführung von technisch organisatorischen Maßnahmen die Umsetzung sämtlicher Vorgaben. Im Bereich der Lösch-/ und Aufbewahrungsfristen ist § 7 Abs. 2 S. 4 AÜG zur Aufbewahrung von Geschäftsunterlagen für die Dauer von drei Jahren zu beachten. Eine Vereinbarung zur gemeinsamen Verantwortlichkeit gem. Art. 26 DS-GVO kann viele Konstellationen der Arbeitnehmerüberlassung abbilden, um die jeweiligen Pflichten der Vertragsparteien gegenüber den Leiharbeitnehmer*innen vertraglich zu normieren. Eine Vereinbarung zur Auftragsverarbeitung nach Art. 28 DS-GVO kommt allerdings in der Regel nicht in Betracht.*

[40] Vgl. zur Personalvermittlung auch: DSK Kurzpapier Nr. 16 zu gemeinsamer Verantwortlichkeit, Art. 26 DSGVO, Stand: 19.03.2018

III. Fall 14: 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 vergangenen Jahre zu präsentieren. Arbeitsvertragliche Konsequenzen muss er bekanntermaßen nicht mehr befürchten. Und warum nicht den Kollegen zum Abschied etwas 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. Das Unternehmen ist in diesem Fall nämlich als Dienstanbieter im Sinne des TKG bzw. TMG anzusehen und dem Fernmeldegeheimnis unterworfen. Der Zugriff auf die E-Mail-Accounts der Mitarbeiter ist somit unzulässig. Und dies betrifft nicht nur die privaten E-Mails, sondern auch die dienstlichen, wenn diese in dem Account nicht vorab abgegrenzt werden können. 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 sei. Sämtliche Kundenanfragen seien bislang über die ausgeschiedenen Mitarbeiter gelaufen. Nicht mehr auf die E-Mail-Accounts zugreifen zu können, sollte zum Auftragsverlust und angesichts der schwierigen wirtschaftlichen Lage des Unternehmens zur Insolvenz führen.

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:

Davon, ihren Beschäftigten auch die private Nutzung des betrieblichen E-Mail-Systems zu ermöglichen, raten wir Unternehmen grundsätzlich ab. Denn dem – durchaus nachvollziehbaren – Wunsch des Arbeitgebers, die private Nutzung durch den Arbeitnehmer dann aber überprüfen zu wollen, ist in diesem Falle ein Riegel vorgeschoben. Unsere Empfehlung geht deshalb dahin, den Beschäftigten nicht die private Nutzung des betrieblichen E-Mail-Systems zu gestatten, sondern nur die des Internets. Auf diese Weise können die Angestellten ihre privaten E-Mail-Accounts abrufen, ohne den betrieblichen nutzen zu müssen. Dies ermöglicht eine klare(re) Abgrenzung vom privaten zum geschäftlichen Bereich und damit auch einen gegebenenfalls notwendigen Zugriff auf die E-Mails im betrieblichen Account. Da die Ermöglichung der privaten Internetnutzung nicht in unmittelbarem Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses steht, sondern sozusagen eine Zusatzleistung des Arbeitgebers ist, und auch ansonsten nicht für die Erfüllung des Vertrages erforderlich ist, kann die Kontrolle darüber nicht auf § 26 BDSG oder Art. 6 Abs. 1 S. 1 lit. b) DS-GVO gestützt werden. Es muss vielmehr eine Einwilligung eingeholt werden. Die im Beschäftigungsverhältnis oft problematische Freiwilligkeit der Einwilligung kann hier in der Regel durch § 26 Abs. 2 S. 2 BDSG hergestellt werden. Es ist außerdem ratsam, in die Einwilligungserklärung ganz explizit die Zwecke der Speicherung aufzunehmen, ebenso wie den Zeitraum der Speicherung und eventuelle Löschfristen, in welchem zeitlichen Abstand Kontrollen erfolgen sollen und wer Zugriff auf die gespeicherten Daten haben wird. Es sollte auch genauer erläutert werden, was der Arbeitgeber unter einer „angemessenen" Nutzung versteht, also beispielsweise der Umfang oder ein Zeitrahmen angegeben werden, in dem die private Nutzung (nur) stattfinden darf.

Wie lange personenbezogene Daten (meist in Dokumenten oder Akten) aufzubewahren sind, bevor eine Löschung vorgenommen werden kann, ist abhängig von deren Inhalt und Zweck. Für Unterlagen, die für die Besteuerung des Unternehmens relevant sind, geben die steuerrechtlichen Vorschriften eine Aufbewahrungszeit von sechs oder zehn Jahren vor (vgl. § 147 Abgabenordnung oder auch § 257 Handelsgesetzbuch). Arbeitszeitnachweise sind zwei bzw. drei Jahre aufzubewahren, damit die Einhaltung von Arbeitszeitregelungen nachgewiesen werden kann. Auch besteht die Möglichkeit, dass nach Beendigung des Beschäftigungsverhältnisses weitere Ansprüche geltend gemacht werden, z.B. 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 drei Jahren. Dabei beginnt gemäß § 199 BGB die Frist erst mit dem Ende des Jahres, in dem der Anspruch entstanden ist.

***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.

D. Das Ziel unserer Arbeit

Wie die kleine Auswahl aus dem Bereich des Beschäftigtendatenschutzes zeigt, 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 Augenmerk auch weiterhin besonders auf die datenschutzrechtliche Beratung. Der Aufgabenkatalog aus Art. 57 Abs. 1 DS-GVO 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.[41] 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 auch gemeinsam datenschutzkonforme Lösungen und Alternativen zu erarbeiten.

[41] Vgl. Art. 57 Abs. 1 lit. b) und d) DS-GVO.

Schlagwort	Stichworte	Kurz-Erläuterung	Quellen
Abmahnung	Entfernung einer Abmahnung aus der Personalakte	Mangels Rechtsschutzbedürfnisses hat ein ehemaliger Arbeitnehmer keinen Anspruch auf Entfernung einer Abmahnung aus der Personalakte; es sei denn, die Abmahnung erging zu Unrecht (dann Löschungsanspruch nach §§ 242, 1004 BGB analog).	BAG, Urt. v. 11.01.2001 – 9AZR 464/00; LAG Schleswig-Holstein, 19.07.2016 – 1 Sa 37/16
Arbeitgeber-verbände / Gewerkschaften	Datenübermittlungen an Arbeitgeberverbände und Gewerkschaften	Personaldatenübermittlungen an Arbeitgeberverbände oder Gewerkschaften bedürfen der ausdrücklichen Einwilligung der Arbeitnehmer. Eine Satzung, welche den Einzug des Gewerkschaftsbeitrags per Gehaltsabzug festlegt, stellt keine ausreichende Rechtsgrundlage dar. Die Übertragung in Form von anonymisierten Lohnlisten zur Überprüfung der Gehaltssituation durch die Gewerkschaft ist ohne Einwilligung zulässig.	LDI NRW, TB 2007, Ziff. 14.2; Gola, Handbuch BeschDS 2019, Rn. 1021 ff.; Däubler, Gläserne Belegschaften, Rn. 456
Background-Checks	Zur Zulässigkeit sogenannter Pre-Employment-Checks	Der LfDI BW empfiehlt, auf die Durchführung dieser Screenings zu verzichten. Den Verantwortlichen würden zudem wegen Art. 14 DS-GVO umfangreiche Informations-pflichten treffen. Zulässige Ausnahme: Abgleich mit EU-Terrorverdachtsliste (Rechtsgrundlage: § 26 Abs. 1	LfDI BW, Ratgeber Beschäftigten-Datenschutz 2019, Fall 4, S. 30; Terrorlisten-Abgleich: BFH, Urt. v. 19.06.2012, VII

		BDSG i.V.m. § 34 Abs. 4 AWG).	R 43/11
Beschäftigten-datenschutz	§ 26 Abs. 8 BDSG	Der Beschäftigtendatenschutz des BDSG erstreckt sich auf natürliche Personen, die in einem der in § 26 Abs. 8 BDSG beschriebenen Beschäftigungsverhältnis stehen und deren Daten zu Zwecken dieser Vertragsbeziehung verarbeitet werden.	Gola, Handbuch BeschDS 2019, Rn. 219
Beschäftigten-daten-verarbeitung	Öffnungsklausel Art. 88 i.V.m § 26 BDSG	Art. 88 Abs. 1 DS-GVO öffnet spezialgesetzliche Regelungen der Mitgliedsstaaten, davon wurde in Deutschland in Form des § 26 BDSG Gebrauch gemacht. Dieser präzisiert und verdrängt Art. 6 Abs. 1 Buchst. b) DS-GVO. Die sonstigen Zulässigkeitsregelungen aus Art. 6 und 9 DS-GVO werden nicht tangiert.	Schulz in: Gola, DS-GVO, Art. 6, Rn. 34 ff.
Betriebliches Eingliederungsmanagement (BEM)	BEM nur mit Einwilligung des betroffenen Beschäftigten	Gemäß § 167 Abs. 2 S. 1 SGB IX muss der Betroffene in die Durchführung des BEM-Verfahrens einwilligen. Die Einwilligung muss die Voraussetzungen der Art. 7 und Art. 9 Abs. 2 Buchst. a DS-GVO erfüllen.	Däubler, Gläserne Belegschaften, Rn. 399b f.
Betriebsarzt	Limitierte Datenweitergabe des Betriebsarztes an den Arbeitgeber	Die Verarbeitung ist gem. § 22 Abs. 1 Nr. 1 lit. b BDSG erlaubt, wenn dies "zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten […] erforderlich ist." Der Betriebsarzt hat jedoch die ärztliche Schweigepflicht zu beachten (§ 8 Abs. 1 S. 3 ASiG), wenn er sich nicht gemäß § 203 StGB strafbar machen möchte. Der	BAG, Urt. v. 12.09.2006 – 9 AZR 271/06; OLG Düsseldorf, Urt. v. 11.12.2008 – I-15 U 170/07, Rn. 71 m.w.N.

		Betriebsarzt darf dem Arbeitgeber lediglich mitteilen, ob ein Arbeitnehmer für eine bestimmte Arbeitsaufgabe geeignet, beschränkt geeignet oder nicht geeignet ist (beschränkt auf das Ergebnis der Untersuchung). Einen Anspruch auf Auskunft über die Art der Erkrankung hat der Arbeitgeber nicht. Akten des Betriebsarztes sind keine Unterlagen des Arbeitgebers und gehören nicht in die Personalakte.	
Betriebsrat	Betriebsrat als Verantwortliche r	Der Betriebsrat handelt bei der im Rahmen seiner Aufgaben stattfindenen Verarbeitung von Beschäftigtendaten in eigener Verantwortlichkeit.	LfDI BW, 34. Tätigkeitsbericht (2018), Abschnitt 1.6.1 Nr. 3; LAG Niedersachsen, Beschl. v. 22.10.2018 – 12 TaBV 23/18; LAG Sachsen-Anhalt, Beschl. v. 18.12.2018 – 4 TaBV 19/17; ablehnend: LAG Hessen, Beschl. v. 10.12.2018 – 16 TaBV 130/18
Betriebs-übergang	Datenübermittl ungen bei Unternehmens verkauf/-übernahme / Insolvenz	Da der neue Betriebsinhaber an die Stelle des bisherigen Arbeitgebers tritt, ist die Datenübermittlung (Personalinformationen) gemäß § 26 Abs. 1 S. 1 BDSG zur Durchführung des übergeleiteten Arbeitsvertrags erforderlich. Die Vorschrift gilt	BAG, Urt. v. 30.10.1986 – 2 AZR 101/85; Maschmann, Betriebs-Berater (BB) 2019, 628-636 m.w.N.

		für den Insolvenzverwalter entsprechend.	
Betriebsvereinbarung / Dienstvereinbarung	Rechtssetzungs-befugnis von Betriebsräten/Personalräten	Kollektivvereinbarungen erzeugen als „Gesetz des Betriebs“ objektives Recht, welche als Rechtsgrundlage zur Verarbeitung von Beschäftigtendaten dienen (können), Art. 88 DS-GVO i.V.m. § 26 Abs. 1 BDSG oder § 15 LDSG BW; auch Daten besonderer Kategorien (Art. 9 DS-GVO, § 26 Abs. 4 BDSG). Das Schutzniveau der DS-GVO darf jedoch nicht unterschritten werden.	Däubler, Gläserne Belegschaften, Rn. 783 b; Maschmann in: Kühling/Buchner, DS-GVO/BDSG, Art. 88 Rn. 40; Pötters in: Gola, DS-GVO, Art. 88, Rn. 18ff m.w.N.
Bewerbungs-unterlagen	4-monatige Speicherfrist von Bewerbungs-unterlagen	Der LfDI BW hält eine Speicherung von Bewerbungsunterlagen nach Abschluss des Auswahlverfahrens über vier Monate hinaus für nicht erforderlich und empfiehlt Arbeitgebern, nach Ablauf dieser Zeitspanne eine (automatische) Löschung zu veranlassen.	LfDI BW, Ratgeber Beschäftigten-Datenschutz 2019, Fall 6, Seite 31 f.
Bring your own Device (BYOD)	Nutzung von privaten IT-Geräten (Handy, Laptop) oder Software	Die Nutzung von privater digitaler Technik bedarf einer gesonderten Vereinbarung (z.B. Betriebs-vereinbarung). Der Arbeitgeber ist auch für diese Geräte/Software Verantwortlicher und hat alle Pflichten der DS-GVO einzuhalten (insb. Umsetzung technischer und organisatorischer Maßnahmen). Das Kontrollrecht des LfDI umfasst auch das dienstlich	Klein-Henning in: Schläger/Thode. Handbuch Datenschutz, Teil I, Rn. 230 ff.; Söbbing, Rechtsrisiken durch BYOD, RDV 2013, 77; Gola, Handbuch BeschDS 2019, Rn. 1110 ff.

		genutzte private Endgerät.	m.w.N.
Daten-verarbeitung	Zulässigkeit von Daten-verarbeitungen	Entgegenstehende schutzwürdige Interessen des Arbeitnehmers machen eine Datenverarbeitung nicht grundsätzlich unzulässig.	Gola, Handbuch BeschDS 2019, Rn. 57
Dienstjubiläum	Gratulation zu Dienstjubiläen	Soll durch die Behördenleitung, den direkten Vorgesetzten oder die Personalabteilung eine Gratulation zum Dienstjubiläum, Geburtstag etc. erfolgen, ist keine Einwilligung notwendig. Rechtsgrundlage hierfür bildet Art. 6 Abs. 1 S. 1 Buchst. f) DS-GVO (Pflege des Betriebsklimas). Soll aber das Ereignis „betriebsöffentlich“ (z.B. im Intranet) bekannt gegeben werden, und / oder die Gratulation aus der Abteilung / dem Kollegium “heraus“ erfolgen (z.B. durch Grußkarte der gesamten Abteilung), bedarf dies der vorherigen Einwilligung.	Zehnter Bericht Aufsichtsbehörde Hessen, RDV 1998, 271; Gola, Handbuch BeschDS 2019, Rn. 479, 892; Däubler, Gläserne Belegschaften, Rn. 484
Einwilligung im Beschäftigungs-verhältnis	Art. 7 DS-GVO, § 26 Abs. 2 BDSG, Erwägungsgrund 155	Grundsätzlich dürfen personen-bezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung der Beschäftigten verarbeitet werden. Problematisch ist jedoch oftmals die Frage, ob die Einwilligung freiwillig erteilt wurde. Fälle in denen eine Freiwilligkeit bejaht werden kann sind u.a.: • Veröffentlichung von Mitarbeiter-Fotos • Protokollierung/Kontrolle (Stichproben) des	BT-Drs. 18/11325 S. 97; Anlage zu BfDI Info Nr. 5: Datenschutz und Telekommu-nikation

		Internetzugangs bei Erlaubnis einer privaten Nutzung am Arbeitsplatz • Aufnahme in Geburtstagsliste	
Geburtstags-liste	Führung einer Geburtstagsliste / Dienstjubiläum	Die Aufnahme in eine solche Liste bedarf stets der Einwilligung des Beschäftigten und kann nie aus anderen Gründen gerechtfertigt sein („Pflege des Betriebsklimas“).	10. Bericht Aufsichtsbehörde Hessen, RDV 1998, 271
Geburtstags-liste betriebsintern veröffentlichen	Betriebsinterne Veröffentlichung einer Geburtstagsliste	Die Aufnahme in eine Geburtstagsliste, welche betriebsintern veröffentlicht werden soll, bedarf der ausdrücklichen Einwilligung des Beschäftigten.	Siehe Nachweise zu „Dienstjubiläum“
GPS-Überwachung im Kfz	Zugang zu Standortdaten von Mitarbeitern durch im Fahrzeug befindliches GPS	Es bedarf eines legitimen Interesses, solche Daten zu erheben: z.B. Lokalisation bei Autodiebstahl/ Unfall. Es muss das mildeste Mittel gewählt sein: im Beispiel darf der Sender erst aktiviert werden, wenn ein solcher Fall vorliegt. Auf jeden Fall muss eine (grundlose) Rundumkontrolle ausgeschlossen sein. Allgemeine Überwachungen zur Kontrolle des Verbots privater Nutzung oder zur Ermittlung von Umwegfahrten sind unverhältnismäßig (milderes Mittel: manuelles Fahrtenbuch). Anerkannt ist die GPS-Ortung von Geldtransportern.	LDI NRW, 20. TB (2009/2010), Ziff. 7.6; LfD Niedersachsen, 21. TB (2009/2010), S. 31; Gola, Handbuch BeschDS 2019, Rn. 1273 ff.
Interessen-ausgleich	Art. 6 Abs. 1 Satz 1 Buchstabe f	Im Rahmen der Erforderlichkeits-prüfung sind die widerstreitenden	Pötters in: Gola, DS-GVO, Art. 88, Rn. 47 ff.

	DS-GVO	Grundrechtspositionen abzuwägen. Dabei ist das informationelle Selbst-bestimmungsrecht des Beschäftigten (Art. 1 Abs. 1, Art. 2 GG) mit dem Eigentumsrecht (Art. 14 Abs. 1 GG), der unternehmerischen Freiheit (Art. 12 GG) und der Vertragsfreiheit des Arbeitgebers (Art. 2 Abs. 1 GG) auszugleichen.	und Gola, Handbuch BeschDS 2019, Rn. 142
Konzern-Personaldaten	Konzernweite Datenverarbeitung von Beschäftigten-daten	Werden Personaldaten innerhalb eines Konzerns übermittelt, bedarf es einer Rechtsgrundlage. Diese liegt in Art. 6 Abs. 1 S. 1 Buchst. f DS-GVO i.V.m. Erwägungsgrund 48, wobei der konzerninterne Datenaustausch als berechtigtes Interesse für interne Verwaltungszwecke gilt. Bei besonderen Kategorien ist außerdem Art. 9 DS-GVO zu beachten.	Härting, Datenschutz-Grundverordnung 2016
Milderes Mittel	Maßnahme nur erforderlich, wenn mildestes Mittel gewählt	• zur Diebstahlsprävention ist eine stichprobenartige Torkontrolle milder als eine permanente VÜ • Heimliche Spindöffnung nicht verhältnismäßig, da Öffnung auch im Beisein stattfinden könnte	BAG, 15.4.14., 1 ABR 2/13; BAG, 20.6.13 – 2 AZR 546/12
Mitarbeiterfotos	Veröffentlichung von Mitarbeiterfotos	Gemäß Art. 85 DS-GVO i.V.m. § 22 KUG dürfen (Mitarbeiter-) Fotos nur mit Einwilligung des Abgebildeten verbreitet werden. Gleiches gilt für sog. Image-Filme.	BGH, Urt. v. 26.01.1971 – VI ZR 95/70; BGH, Urt. v. 12.12.1995 – VI ZR 223/94
Mitarbeiter-	Konzernweites Namens-,	Ein solches Verzeichnis ist gemäß § 26 Abs. 1 S. 1 BDSG	15. Bericht der Hessischen

verzeichnis	Telefon- und E-Mail-Verzeichnis	zum Zwecke einer schnellen und reibungslosen konzerninternen Kommunikation erlaubt.	Landesregierung über die Tätigkeit der Aufsichts-behörden für den Datenschutz im nichtöffentlichen Bereich vom 26.11.2002 (LT-Drs. 15/4659 = RDV 2003)
Personalakten-einsicht	Einsichtsrecht in die Personalakte eines ehemaligen Mitarbeiters	Unabhängig von der Geltendmachung eines berechtigten Interesses, hat auch ein ausgeschiedener Arbeitnehmer Anspruch auf Einsicht in seine (noch vorhandene) Personalakte. Dies ergibt sich aus § 241 Abs. 2 BGB.	BAG, Urt. v. 16.11.2010 – 9 AZR 573/09 = NZA 2011, 453
Personalrabatt	Erfassung von Personal-einkäufen	Wenn der Arbeitgeber die rabattierten Einkäufe erfassen muss, um festzustellen, ob der steuerliche Freibetrag („geldwerter Vorteil“) überschritten wurde, ist eine Datenerhebung nach § 26 Abs. 1 S. 1 BDSG (zu Zwecken der Entgeltberechnung) gerechtfertigt.	30. Tätigkeits-bericht des LfD Baden-Württemberg (2010/2011), S. 140f
Polizeiliches Führungs-zeugnis	Anforderung eines Führungszeugnisses vor Beschäftigungs-beginn	Eine solche Datenerhebung kann erforderlich sein für Bewerber auf „Vertrauenspositionen“ (z.B. Lagerverwalter), bei denen Konflikte mit dem Strafgesetz relevant sein können oder deren besondere Zuverlässigkeit von zentraler Bedeutung ist. Eine Einwilligung ist mangels	Gola, Handbuch BeschDS 2019, Rn. 676; Kort, NZA-Beilage 2/2016, S. 69

		Freiwilligkeit keine taugliche Rechtsgrundlage für die Datenerhebung.	
Schwerbehinderung	Keine Pflicht zur Preisgabe des Schwerbehinderungsstatus im Bewerbungs-verfahren	Der Status „Schwerbehinderung“ stellt eine besonders schützenswerte Gesundheitsinformation i.S.d. Art. 9 Abs. 1 DS-GVO dar. Die Angabe im Personalfragebogen muss als freiwillig gekennzeichnet sein. Dem behinderten Bewerber muss freigestellt sein, ob er den ihm gewährten Schutz aus AGG und § 81 SGB IX bereits im Bewerbungsverfahren in Anspruch nehmen will.	BAG, Urt. v. 18.09.2014 – 8 AZR 759/13
Videointerview	Videointerviews statt Bewerbungs(vor)gespräch	Erfolgt das Interview live und werden Bild und Ton nicht aufgezeichnet, bestehen keine datenschutzrechtlichen Bedenken. Ob der Bewerber in eine Aufzeichnung freiwillig einwilligen kann, ist aufgrund der besonderen Spannungssituation sehr fraglich.	BfDI Berlin, Jahresbericht 2016, Ziff. 7.3, S. 117
Videoüberwachung	Videoüberwachung (VÜ) am Arbeitsplatz – Unterteilt nach verdeckter und offener VÜ	Der Einsatz einer versteckten (den Beschäftigten unbekannte) Kamera ist grds. unzulässig (Ausnahme in sehr engen Grenzen: begründeter Verdacht einer Straftat gegen den Arbeitgeber). Ist die Kamera darauf gerichtet, ausschließlich das Arbeitsverhalten der Beschäftigten festzuhalten oder so eingestellt, dass diese jederzeit ohne Kenntnis der Beschäftigten eingeschaltet	BAG, Urt. v. 25.04.2017 – 1 ABR 46/15; zu Kameras in Supermärkten siehe: BAG 23.08.2018 – 2 AZR 133/18

		werden kann, stellt dies eine unzulässige „Totalkontrolle“ dar. Erfolgt die VÜ offen, sind zwar weniger strenge Maßgaben zu beachten, dennoch darf die VÜ nicht so ausgestaltet sein, dass die Arbeitsplätze der Beschäftigten dauerhaft überwacht werden (und damit einer – unzulässigen - Verhaltenskontrolle gleichlaufen).	
Whistleblowing (intern)	Meldung von Verstößen durch Arbeitskollegen (sog. interner Whistleblower / Hinweisgeber)	Die Datenverarbeitung kann gemäß § 26 Abs. 1 S. 2 BDSG rechtmäßig sein, um bei Durchführung des Beschäftigungs-verhältnisses Straftaten und Rechtsverstöße aufzudecken. Dem Verantwortlichen treffen jedoch die Info-Pflichten nach Art. 13, 14 DS-GVO, deshalb ist die Zulässigkeit anonymer Anzeigen höchst problematisch und wird nicht aufrecht zu erhalten sein.	Borchers in: Schläger/Thode, Handbuch Datenschutz 2018, Teil C, Rn. 328 f; Gola, Handbuch BeschDS 2019, Rn. 786ff.
Zeiterfassung	Automatisierte Verarbeitung (Erfassung) von Krankheits- und Fehlzeiten verstößt nicht gegen Art. 22 DS-GVO	Es ist ein berechtigtes Interesse des Arbeitgebers, sich diejenigen Kenntnisse schnell und kostengünstig zu verschaffen, die er benötigt um festzustellen, inwieweit die Arbeitsleistung durch Krankheits- und Fehlzeiten gestört ist. Er darf ein automatisiertes System verwenden, auch wenn er dies ohne technische Hilfsmittel schaffen könnte.	EuGH, Urt. v. 14.05.2019 – C 55/18; BAG, Urt. v. 11.03.1986 – 1 ABR 12/84 = NJW 1986, 2724

Zugangskontrollsystem	Codierte Werksausweise als Schlüssel zum Betrieb	Es bestehen keine datenschutzrechtlichen Bedenken gegen ein Zugangskontrollsystem, solange der Werksausweis/Chip lediglich als Schlüssel fungiert und das System nicht dafür genutzt wird, um das Verhalten oder die Leistung der Beschäftigten zu überwachen.	BAG, Urt. v. 10.04.1984 – 1 ABR 69/82; Däubler, Gläserne Belegschaften, Rn. 732