DSGVO-INFO

DIE UMFASSENDE INFORMATIONSPLATTFORM

STIFTUNG DATENSCHUTZ

BESCHÄFTIGTENDATENSCHUTZ

Juli 2020

Prof. Dr. Anne Riechert

Inhaltsverzeichnis

Stand: Juli 2020
Autorin: Prof. Dr. Anne Riechert

I. Grundsätze

1. Welche Gesetze regeln den Datenschutz für Beschäftigte?

Die **Datenschutzgrundverordnung** (DSGVO) enthält eine Öffnungsklausel für eine eigenständige nationale Regelung im Beschäftigungskontext. Von dieser Regelungskompetenz hat der deutsche Gesetzgeber im Rahmen des § 26 **Bundesdatenschutzgesetz** (BDSG) auch Gebrauch gemacht. Diese Regelung ist allerdings inhaltlich nahezu identisch mit § 32 BDSG-alt. Kritik wird daran geübt, dass der deutsche Gesetzgeber bislang darauf verzichtet hat, ein einheitliches Beschäftigtendatenschutzgesetz zu kodifizieren.

Aktuell wurde vom Bundesministerium für Arbeit und Soziales der „Beirat Beschäftigtendatenschutz" berufen, welchem die Verfasserin dieser Handreichung als Mitglied angehört. Hintergrund ist der Koalitionsvertrag, der vorsieht, die Öffnungsklausel der europäischen Datenschutzgrundverordnung zu nutzen und die Schaffung eines eigenständigen Gesetzes zum Beschäftigtendatenschutz zu prüfen. Der interdisziplinäre Beirat unter Leistung der ehemaligen Justizministerin Frau Prof. Dr. Herta Däubler-Gmelin wird nun zur Umsetzung dieses Prüfauftrags tätig.

Im Falle von Rechtsstreitigkeiten liegt bei Anwendungs- und Auslegungsfragen der Datenschutzgrundverordnung die abschließende Entscheidungskompetenz im Übrigen beim Europäischen Gerichtshof. Ein Gericht eines Mitgliedstaates ist zur Vorlage beim Europäischen Gerichtshof verpflichtet (Vorlageentscheidung), wenn dessen Entscheidung selbst nicht mehr mit Rechtsmitteln des innerstaatlichen Rechts angefochten werden kann.

2. Für wen gilt das Gesetz?

Das Gesetz gilt wie unter der bisherigen Rechtslage für Beschäftigte. Dieser Begriff der „Beschäftigten" ist umfassender als der Begriff des „Arbeitnehmers" und wird wie folgt definiert:

- Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer im Verhältnis zum Entleiher zu ihrer Berufsbildung Beschäftigte,
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
- in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
- Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz oder dem Bundesfreiwilligendienstgesetz leisten,
- Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten ebenso als Beschäftigte. Es wurde außerdem klargestellt, dass die Beschäftigteneigenschaft von Leiharbeitnehmern gleichermaßen im Verhältnis zum Entleiher gilt (und nicht nur zum Verleiher). Insgesamt beinhaltet dies keine Änderung zu der bisherigen Rechtslage.

In Kürze:
Es fallen alle Beschäftigungsverhältnisse unter diese Regelung und sie bezieht sich ebenso auf Leiharbeiter, Auszubildende und Zivildienstleistende. Keine Geltung hat das Bundesdatenschutzgesetz für Beamtinnen und Beamte - auch wenn darauf Bezug genommen wird. Für Bedienstete und Beschäftigte bei Behörden und öffentlichen Stellen des Bundes und Länder sowie der Kommunen finden vielmehr besondere (u.a. beamtenrechtliche) bundes- und landesspezifische Regelungen Anwendung.

3. Automatisierte und nicht-automatisierte Verarbeitung der Beschäftigtendaten

Die Datenschutzgrundverordnung gilt für die ganz oder teilweise **automatisierte** Verarbeitung personenbezogener Daten sowie für die **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem Dateisystem **gespeichert sind oder gespeichert werden sollen**. Ein Dateisystem stellt eine strukturierte Sammlung personenbezogener Daten dar, die nach bestimmten Kriterien (z.B. Datum, alphabetische Reihenfolge) geordnet ist.

Beispiel: Dateisystem

Ein Dateisystem stellt eine strukturierte Sammlung personenbezogener Daten dar, die nach bestimmten Kriterien (z.B. Datum, alphabetische Reihenfolge) geordnet ist. Die DSGVO findet daher auch bei nichtautomatisierter Datenverarbeitung Anwendung, wenn eine Unternehmerin einen Ordner mit handschriftlichen Notizen über ihre Kunden anlegt - vorausgesetzt, sie legt den Ordner strukturiert an (beispielsweise nach Kalenderjahren sowie Geschäftssitz der Unternehmen unterteilt und in alphabetischer Reihenfolge).

Im **Beschäftigtenkontext** würde es hingegen ausreichen, wenn die Arbeitgeberin handschriftliche Vermerke über ihre MitarbeiterInnen unsortiert und in zufällig gewählter Reihenfolge in einem Ordner abheftet.

Zu beachten ist:
Im Beschäftigtenkontext gilt abweichend, dass es ausreichend ist, wenn personenbezogene Daten von Beschäftigten verarbeitet werden, ohne dass diese in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Dies gilt auch für besondere Kategorien personenbezogener Daten (etwa sensible Daten wie Gesundheitsdaten). Davon umfasst sind alle vorstellbaren Handlungsformen, beispielsweise tatsächliche Handlungen wie das Beobachten von Beschäftigten, mündliche Äußerungen oder handschriftliche Notizen über Beschäftigte.

4. Der Betriebsrat

Derzeit besteht Uneinigkeit im Hinblick auf die Frage, inwieweit der Betriebsrat eine „andere Stelle“ und damit selbst Verantwortlicher im Sinne von Artikel 4 Nr. 7 DSGVO ist oder er – wie unter bisherigem Recht – Teil der verantwortlichen Stelle bleibt. Damit ist ebenso die Frage verbunden, ob er weiterhin der Kontrolle durch den betrieblichen Datenschutzbeauftragten sowie der Aufsichtsbehörden entzogen ist. Dies ist noch nicht abschließend entschieden. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ist etwa der Auffassung, dass die gewichtigeren Argumente dafür sprechen würden, dass der Betriebsrat selbst über die konkreten Mittel der Verarbeitung personenbezogener Daten entscheidet (https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/5000/16_5000_D.pdf , S. 37). Dies entspricht ebenso der Ansicht des LAG

Sachsen-Anhalt (Beschluss vom 18.12.2018, abrufbar unter http://www.landesrecht.sachsen-anhalt.de/jportal/portal/t/buq/page/bssahprod.psml?doc.hl=1&doc.id=JURE190003353&showdoccase=1&doc.part=L&paramfromHL=true). Das LAG Hessen hingegen stuft den Betriebsrat lediglich als Teil der verantwortlichen Stelle ein (Beschluss vom 10.12.2018, abrufbar unter https://www.rv.hessenrecht.hessen.de/bshe/document/LARE190005127).

Letzteres entspricht der überwiegenden Meinung in der Literatur. So wird im Hinblick auf die Einordnung als verantwortliche Stelle der Einwand erhoben, dass der Arbeitgeber über die Zwecke und Mittel entscheide, da er regelmäßig auch die entsprechenden IT-Strukturen vorgebe und der Betriebsrat diese nutzen könne (*Wybitul*, Betriebsrat selbst für Datenschutz verantwortlich: Sorgen Datenschutzbehörden bald für Paukenschlag?,https://efarbeitsrecht.net/betriebsrat-selbst-fuer-datenschutz-verantwortlich/). In der Literatur wird außerdem die Auffassung vertreten, dass der Betriebsrat wie auch etwa eine einzelne Abteilungen eines Unternehmens stets nur Teil der verantwortlichen Stelle sein könnten, da ihnen die Rechtsfähigkeit fehlt. Dies ist insoweit überzeugend, da im Rahmen der ehrenamtlichen Tätigkeit des Betriebsrates (§ 37 BetrVG) die Mittelverwendung vom Arbeitgeber abhängt (§ 40 Absatz 2 BetrVG). Insgesamt sind jedoch Entscheidungen der Rechtsprechung abzuwarten.

Aus Sicht der Beschäftigten wichtig:
Wenn der Betriebsrat personenbezogene Daten verarbeitet (z.B. durch Einsichtnahme in Bruttoentgeltlisten), muss er die Regelungen der DSGVO beachten und einhalten!

5. Die Datenschutzbeauftragte

Seit Inkrafttreten der Datenschutzgrundverordnung gibt es auf europäischer Ebene eine Bestellpflicht für Datenschutzbeauftragte, etwa bei umfangreicher Verarbeitung sensibler Daten. Der deutsche Gesetzgeber hat darüber hinaus von der Öffnungsklausel in der DSGVO Gebrauch gemacht und im BDSG eine Pflicht zur Bestellung einer Datenschutzbeauftragten normiert, wenn mindestens 20 Beschäftigte mit der Datenverarbeitung beschäftigt sind (§ 38 BDSG). Den Unternehmen steht es insgesamt frei, die Bestellung intern vorzunehmen (MitarbeiterIn) oder die Position extern zu besetzen.

Zu den Aufgaben eines/einer Datenschutzbeauftragten gehört ebenso die Sensibilisierung und Schulung der MitarbeiterInnen. Außerdem können sich Beschäftigte in Datenschutzfragen an die Datenschutzbeauftragte wenden, da diese gleichermaßen die Interessen der betroffenen Personen vertritt. Eine Datenschutzbeauftragte ist zudem zur Verschwiegenheit verpflichtet.

Für Beschäftigte gilt daher:

MitarbeiterInnen als interne Datenschutzbeauftragte unterliegen einem besonderen Kündigungsschutz und können während ihrer Tätigkeit nur aus wichtigem Grund gekündigt werden. Dies gilt auch nach Ende der Tätigkeit als Datenschutzbeauftragte für einen Zeitraum von einem Jahr, so dass innerhalb eines Jahres eine ordentliche Kündigung unzulässig ist.

Dieser Kündigungsschutz ist jedoch an die gesetzliche Verpflichtung zur Bestellung einer Datenschutzbeauftragten gekoppelt.

Beispiel: Freiwillige Bestellung von Datenschutzbeauftragten

Ein Unternehmen hat 20 Beschäftigte, aber davon sind lediglich zehn MitarbeiterInnen mit der Verarbeitung personenbezogener Daten beschäftigt, in dem ihnen Zugriffsrechte auf die Kundendatenbank eingeräumt wurden. In diesem Falle besteht zwar nach BDSG keine Verpflichtung zur Bestellung eines Datenschutzbeauftragten, aber das Unternehmen kann die Bestellung auf freiwilliger Basis vornehmen. In diesem Falle genießt der Datenschutzbeauftragte allerdings keinen besonderen Kündigungsschutz.

Nach der Rechtsprechung des Bundesarbeitsgerichts soll dieser Kündigungsschutz ebenso entfallen, wenn die Zahl derjenigen, die mit der Datenverarbeitung beschäftigt sind, unter die gesetzlich vorgegebene Anzahl sinkt (siehe hierzu, allerdings noch zur Gesetzeslage unter der alten Fassung des Bundesdatenschutzgesetzes, Bundesarbeitsgericht, Urteil v. 05.12.2019, Az.: 2 AZR 223/19, abrufbar unter https://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&az=2%20AZR%20223/19.

Allerdings hat die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen darauf hingewiesen, dass sich durch Kurzarbeit an der Benennungspflicht nach dem BDSG sich nichts ändert. Die gesetzliche Formulierung des § 38 Abs. 1 BDSG, dass Personen „in der Regel (…) ständig“ mit der Verarbeitung personenbezogener Daten beschäftigt sind, bedeute nicht, dass kurzzeitige Veränderungen berücksichtigt werden, sondern dass es auf eine langfristige Betrachtung ankommt. Es bleibt also während der Kurzarbeit bei der Pflicht zur Benennung eines Datenschutzbeauftragten, **wenn voraussichtlich auch nach einer zeitlich begrenzten Kurzarbeit mindestens 20 Personen mit Datenverarbeitung beschäftigt sein werden** (siehe unter https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/DSB-Kurzarbeit/Kurzarbeit-_-ohne-Datenschutzbeauftragte-geht-es-nicht.html).

II. Zulässigkeit der Datenverarbeitung

1. Voraussetzungen

Der Arbeitgeber darf im Rahmen eines Beschäftigungsverhältnisses Daten der Beschäftigten verarbeiten, sofern dies **erforderlich** ist

- für die Entscheidung über die Begründung eines Arbeitsverhältnisses oder
- dessen Durchführung oder
- Beendigung oder
- zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten

Der letzte Punkt nimmt nun ausdrücklich auf eine Datenverarbeitung zur Ausübung oder Erfüllung der sich aus einer Kollektivvereinbarung (Tarifvertrag, Betriebs- oder Dienstvereinbarung) ergebenden Rechte und Pflichten Bezug. Eine solche Vereinbarung darf jedoch nicht das Schutzniveau der DSGVO absenken. Hierauf wird gleichfalls von Seiten der Gewerkschaften verwiesen. Als verbindliche Vorgabe enthält die

DSGVO diesbezüglich, dass die Regelungen einer Kollektivvereinbarung geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen müssen.

Zu beachten ist:
Arbeitgeber und Betriebsrat müssen aufgrund der erhöhten Anforderungen ihre Betriebsvereinbarungen überprüfen und gegebenenfalls anpassen oder neu vereinbaren. Besonderes Augenmerk ist dabei auf eine ausreichende Transparenz sowie auf die konkrete und bestimmte Benennung des Zwecks der Verarbeitung und die Festlegung geeigneter und besonderer Schutzmaßnahmen zu legen. Die Datenschutzgrundverordnung nimmt hierauf ausdrücklich Bezug und eine Betriebsvereinbarung darf das Schutzniveau nicht absenken. Umstritten ist, ob eine Betriebsvereinbarung die Regelungen der Datenschutzgrundverordnung verschärfen dürfen. Als Argument gegen eine Verschärfung wird auf die angestrebte Vollharmonisierung verwiesen.

- **Erforderlichkeit der Datenverarbeitung**

Bei dem Merkmal der **Erforderlichkeit** handelt es sich um einen unbestimmten Rechtsbegriff, der der Auslegung bedarf. Es muss folglich eine Verhältnismäßigkeitsprüfung vorgenommen werden und die Datenverarbeitung muss einen legitimen Zweck verfolgen, der nicht mit einem milderen Mittel erreicht werden kann. Insoweit gibt es keinen Unterschied zwischen der alten und der neuen Rechtslage. So kann der Arbeitgeber nach wie vor für die Zwecke der Durchführung des Arbeitsverhältnisses die Stammdaten (Name, Adresse, Bankverbindung, Qualifikation) der Beschäftigten verarbeiten. Weiterhin kann im Rahmen computergestützter Arbeit beispielsweise die Speicherung der Anmeldedaten am Rechner erforderlich sein. Eine Einschränkung der zulässigen Datenverarbeitung kann sich beim Einsatz von IT-Systemen jedoch ergeben, wenn ein milderes Mittel zur Verfügung steht. Nach der Rechtsprechung des Bundesarbeitsgerichts liegt eine unzulässige Datenverarbeitung vor, wenn etwa eine Software eingesetzt wird, die sämtliche Eingaben des Nutzers über die Tastatur protokollieren kann („Keylogger“) oder seine einzelnen Arbeitsschritte erfasst und auswertet. Damit wäre eine lückenlose Überwachung des Beschäftigten möglich.

Es können im Übrigen Bußgelder verhängt werden, wenn der Arbeitgeber Daten der Beschäftigten unrechtmäßig verarbeitet. So hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit kürzlich ein Bußgeldverfahren gegen einen Konzern eingeleitet, da umfangreiche Informationen, die sensible Daten über die Beschäftigten enthielten, anlasslos aufgezeichnet und in Ordnern abgespeichert wurden.

Die Frage der Erforderlichkeit bedarf stets einer Abwägung, wie die nachfolgenden Beispiele zeigen:

> ***Beispiel Fahrerlaubnis***
> Die Arbeitgeberin darf bei Überlassung eines Firmenfahrzeugs die Fahrerlaubnis kontrollieren. Es ist aber nicht erforderlich, zu diesem Zweck eine Kopie des Führerscheins in der Personalakte zu speichern. Zielführender ist es seitens der Arbeitgeberin, sich in regelmäßigen Abständen die Fahrerlaubnis vorlegen zu lassen.

> ***Beispiel Namensschilder***
> Im Einzelhandel kann das Tragen von Namensschildern der Beschäftigten dazu beitragen, eine kundenfreundliche Atmosphäre zu schaffen. Allerdings ist zu diesem Zweck nicht die Angabe des vollständigen Namens erforderlich, sondern der Nachname kann ausreichend sein.

> ***Beispiel Private Internetnutzung***
> Eine Arbeitgeberin darf grundsätzlich überwachen, ob die Beschäftigten das Verbot einer privaten Internetnutzung einhalten. Allerdings muss der Umfang der Kontrollmaßnahmen verhältnismäßig sein. Die Beschäftigten sind daher insoweit geschützt, da keine dauerhafte Überwachung erfolgen darf. Eine solche wäre unverhältnismäßig. Die Arbeitgeberin kann aber Protokolldaten stichprobenartig untersuchen, wobei Aufsichtsbehörden darauf verweisen, dass die Auswertung zunächst ohne Personenbezug vorgenommen werden sollte, d.h. insbesondere ohne Einbeziehung der IP-Adresse und anderer Daten zur Identifizierung der einzelnen Beschäftigten. Ist umgekehrt die Privatnutzung erlaubt, sollten die Beschäftigten nochmals im eigenen Interesse prüfen, inwieweit eine schriftliche Vereinbarung mit der Arbeitgeberin zum Inhalt der gestatteten Privatnutzung vorliegt und diese an Bedingungen geknüpft ist. Die Aufsichtsbehörden weisen darauf hin, dass die Arbeitgeberin eine Einwilligung der Beschäftigten benötigt, die sich auf Art und Umfang von Zugriffen und Kontrollen erstreckt und diese Kontrollen die Einhaltung der vereinbarten Nutzungsregelungen umfassen (z.B. zum zeitlichen Umfang). Die Protokollierung der Internetnutzung durch die Arbeitgeberin bedarf im Übrigen der Zustimmung des Betriebsrats.

Eine Interessenabwägung ist im Übrigen auch für die Verarbeitung besonders sensibler Daten erforderlich, insbesondere bedarf die Einführung von biometrischen Kontrollsystemen durch den Arbeitgeber einer sorgfältigen Verhältnismäßigkeitsprüfung.

> ***Beispiel: Zugangskontrolle mittels Fingerprint***
> Beim Fingerabdruck handelt sich um eine sensible Information. Im Rahmen der Verhältnismäßigkeitsprüfung muss der Arbeitgeber prüfen, ob das schutzwürdige Interesse der betroffenen Personen (der Beschäftigten) an dem Ausschluss der Verarbeitung überwiegt. Der Einsatz eines biometrischen Verfahrens kann erforderlich sein (z.B. wenn es sich um die Zugangskontrolle zu einem Sicherheitsbereich des Unternehmens handelt), bedarf jedoch stets einer besonderen Abwägung.

Wichtig ist außerdem, in die Prüfung stets einzubeziehen, inwieweit ein milderes Mittel in Betracht kommt, das weniger gravierend die Recht der Beschäftigten beschneidet. Dies gilt auch im Bewerbungsverfahren, etwa mit Blick auf Gesundheitsprüfungen oder Einstellungstests.

Zu beachten ist:

In Bezug auf Einstellungstests im Rahmen eines Personalauswahlverfahrens oder ärztlichen Untersuchungen gilt ebenfalls der Grundsatz der **Erforderlichkeit** unter Beachtung und Prüfung eines milderen Mittels. So können beispielsweise ärztliche Bescheinigungen über die gesundheitliche Eignung erforderlich sein, wenn die gesundheitliche Eignung im Einzelfall eine wichtige Voraussetzung darstellt, um den Beruf ausüben zu können, etwa auch zum Schutz von Leben und Gesundheit Dritter (z.B. Pilot).

Bei Eignungstest sollte der Nachweis geführt werden können, dass der jeweilige Test (Arbeitsprobe, Leistungstest, Intelligenztest, Assessments,…) aufgrund seiner konkreten Bewertungsmethode geeignet und erforderlich ist, die Eignung des Bewerbers für die vakante Position festzustellen. Zulässig können nur solche Verfahren sein, die sich in ihrem Inhalt auf die zukünftige Arbeitstätigkeit und den daran gekoppelten Anforderungen beziehen. Allgemeine Intelligenztests zur Erfassung der Gesamtpersönlichkeit des Beschäftigten sind nicht erforderlich und damit unzulässig. Es muss sich insgesamt um einen wissenschaftlich anerkannten Test handeln, der fachkundiger Ausführung bedarf. So müssen psychologische Tests von Psychologen durchgeführt werden, die aufgrund ihrer Schweigepflicht dem Arbeitgeber nur das Gesamtergebnis der Tests übermitteln dürfen (Eignung oder Nichteignung). Das Verfahren muss für den Bewerber transparent sein.

Im Übrigen wurde in der Vergangenheit die Auffassung vertreten, dass Eignungstests nur dann zulässig sein sollen, wenn der Bewerber zugestimmt hat und es sich um die Ermittlung arbeitsbezogener Daten handelt. Nach wie vor bestehen im Arbeitsverhältnis bzw. Bewerbungsverfahren jedoch erhebliche Bedenken im Hinblick auf die Freiwilligkeit der Einwilligung, die gemäß den gesetzlichen Anforderungen zudem transparent und schriftlich erfolgen muss. Grundsätzlich rät der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg davon ab, für die Datenverarbeitung im Bereich des Beschäftigungsverhältnisses (zusätzlich) eine Einwilligung einzuholen (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigtendatenschutz.pdf). Sollte dies dennoch geschehen, empfiehlt er in der Einwilligung explizit darauf hinzuweisen, dass die Datenverarbeitung darüber hinaus auch anhand der gesetzlichen Grundlage erfolgen darf.

- **Berechtigte Interessen?**

Derzeit findet eine Diskussion darüber statt, inwieweit im Rahmen der Verarbeitung von Beschäftigtendaten anstatt des Grundsatzes der Erforderlichkeit ein Rückgriff auf „berechtigte Interessen“ des Arbeitgebers in Betracht kommen kann. Die Auffassungen, die „berechtigte Interessen“ als Legitimationsgrundlage im Beschäftigtenverhältnis ablehnen, verweisen auf den abschließenden Charakter des § 26 BDSG, der die „Erforderlichkeit“ der Datenverarbeitung voraussetzt und gerade nicht auf berechtigte Interessen Bezug nimmt. Die Aufsichtsbehörden nehmen in ihrem Kurzpapier zum „Beschäftigtendatenschutz“ (Kurzpapier Nr. 14, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf) zwar auf eine Interessenabwägung Bezug, führen hierzu jedoch aus, dass eine solche Interessenabwägung den Zusammenhang des neuen Verwendungszwecks zum Beschäftigtenverhältnis berücksichtigen müsse. Daher ist eine Verwendung der Beschäftigtendaten zu gänzlich anderen Zwecken (z.B. Verkauf an Dritte zu Werbezwecken) unter allen Umständen ausgeschlossen.

Zu beachten ist:

Der Arbeitgeber sollte die Verarbeitung der Beschäftigtendaten stets am Maßstab der „Erforderlichkeit" messen. Im Rahmen der praktischen Durchführung können sich außerdem Schwierigkeiten dadurch ergeben, dass der Arbeitgeber zum Nachweis der Rechtmäßigkeit der Datenverarbeitung verpflichtet ist. Diese Rechenschaftspflicht kann im Falle von berechtigten Interessen mit Schwierigkeiten verbunden sein, solange hierzu noch keine anerkannten Fallgestaltungen vorliegen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat allerdings im Zusammenhang mit der Corona-Pandemie ausgeführt, dass aus der Pflicht zur Information des Arbeitgebers über das Vorliegen einer Infektion mit dem Corona-Virus - als eine Nebenpflicht aus dem Arbeitsverhältnis zum Schutz hochrangiger Interessen Dritter - unter gewissen Voraussetzungen auch eine Offenlegungsbefugnis gemäß Artikel 6 Absatz 1 f) DSGVO („berechtigte Interessen") bezüglich personenbezogener Daten der Kontaktpersonen folgen kann (https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html)

- **Konzerninterne Datenübermittlung**

Sollen Daten im Konzern übermittelt werden, ist eine solche Übermittlung nicht privilegiert, sondern es ist hierfür eine Rechtsgrundlage notwendig. In diesem Zusammenhang nimmt die DSGVO auf die „berechtigten Interessen", die in dem vorherigen Punkt behandelt wurden, ausdrücklich Bezug: So heißt es in Erwägungsgrund 48, dass Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse haben *können*, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Hierfür ist eine Interessenabwägung erforderlich, die aufgrund der Rechenschaftspflicht des Verantwortlichen dokumentiert werden muss. Wird die konzerninterne Datenübermittlung in einer Betriebsvereinbarung geregelt, muss diese ebenso rechtmäßig sowie für die Betroffenen nachvollziehbar (transparent) sein und zudem der Zweckbindungsgrundsatz umgesetzt werden.

2. Zur Aufdeckung von Straftaten

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat. Ordnungswidrigkeiten sollen hiervon nicht umfasst sein. Dies bedeutet, dass die Verarbeitung erst erfolgen darf, nachdem die Anhaltspunkte für eine Straftat vorliegen und insgesamt keine Vorsorgemaßnahme erlaubt ist. Eine „Vorratsdatenspeicherung" ist somit unzulässig. Die Aufsichtsbehörden weisen außerdem darauf hin, dass sich die Maßnahmen gegen bestimmte verdächtigte Beschäftigte richten müssen und nicht gegen größere Gruppen von Beschäftigten.

Nicht gesetzlich geregelt ist weiterhin, ob eine Datenverarbeitung bei einem Verdacht einer schwerwiegenden Pflichtverletzung in Betracht kommen kann. Das Bundesarbeitsgericht hat hierzu noch unter der alten Rechtslage entschieden, dass eine vom Arbeitgeber veranlasste verdeckte Überwachungsmaßnahme *zur Aufdeckung eines auf Tatsachen gegründeten konkreten Verdachts einer schwerwiegenden Pflichtverletzung* des Arbeitnehmers zulässig sein kann (Urteil vom 29. Juni 2017-2 AZR 597/16; http://juris.bundesarbeitsgericht.de/zweitesformat/bag/2017/2017-08-30/2_AZR_597-16.pdf). In diesem

Zusammenhang soll ergänzend erwähnt werden, dass gemäß einer weiteren Entscheidung des Bundesarbeitsgerichts die Einsichtnahme in auf einem Dienstrechner der Beschäftigten gespeicherte und nicht als "privat" gekennzeichnete Dateien im Einzelfall sogar als verhältnismäßig eingestuft wird, auch wenn kein begründeter Verdacht einer Pflichtverletzung vorliegt. Das soll nach der Auffassung des Bundesarbeitsgerichts jedenfalls dann gelten, wenn die Überwachungsmaßnahme offen erfolgt und der Arbeitnehmer im Vorfeld darauf hingewiesen worden ist, welche berechtigten Gründe eine Einsichtnahme in - vermeintlich - dienstliche Ordner und Dateien erfordern können (siehe hierzu Bundesarbeitsgericht, Urteil vom 31.1.2019, 2 AZR 426/18 , abrufbar unter http://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=en&nr=22507).

Für Compliance-Maßnahmen und für interne Ermittlungen gilt daher:

An Überwachungsmaßnahmen zur Aufdeckung schwerwiegender Pflichtverletzungen sind wie beim Verdacht einer Straftat hohe Anforderungen zu stellen sind. Gemäß den Ausführungen des Bundesarbeitsgerichts muss ein auf konkrete Tatsachen gegründeter Verdacht für das Vorliegen einer solchen Pflichtverletzung bestehen. Eine dahingehende verdeckte Ermittlung „ins Blaue hinein“, ob ein Arbeitnehmer sich pflichtwidrig verhält, ist unzulässig. Es dürfen außerdem keine milderen und ebenso wirksamen Maßnahmen in Betracht kommen, um den Verdacht aufzuklären. Hierfür ist eine umfassende Abwägung der Interessen des Arbeitnehmers und des Arbeitgebers im Einzelfall erforderlich.

Insgesamt ist jedoch zu berücksichtigen, dass aufgrund des Transparenzgebots der Datenschutzgrundverordnung Zweifel an der Zulässigkeit von Maßnahmen geäußert werden, die sich auf eine schwere Pflichtverletzung beziehen, insbesondere da die ausdrückliche gesetzliche Legitimationsgrundlage fehlt. Daher bleibt abzuwarten, inwieweit die oben zitierte Rechtsprechung des Bundesarbeitsgerichts weiterhin Bestand haben kann. In der Praxis wird daher oftmals empfohlen, Maßnahmen zur Aufdeckung einer schweren Pflichtverletzung in einer Betriebsvereinbarung zu regeln. Folgt man dieser Empfehlung, ist zum einen im Hinterkopf zu behalten, dass auch dies mit der rechtlichen Unsicherheit behaftet ist, ob eine solche betriebliche Regelung zulässig ist. Zum anderen ist - wie oben unter II. 2. „berechtigte Interessen“ bereits ausgeführt - umstritten, inwieweit unter der Datenschutzgrundverordnung überhaupt „berechtigte Interessen“ des Arbeitgebers als Rechtsgrundlage neben den Regelungen des BDSG zum Beschäftigtendatenschutz in Betracht kommen können.

3. Einwilligung

Wegen des Über-/Unterordnungsverhältnisses ist von Einwilligungen im Arbeitsverhältnis grundsätzlich zurückhaltend Gebrauch zu machen. Allerdings wird seitens der Aufsichtsbehörden klargestellt, dass Beschäftigte freiwillig in eine Datenverarbeitung einwilligen können, wenn für sie ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen. Verwiesen wird dabei auf Zusatzleistungen des Arbeitgebers (beispielsweise die private Nutzung dienstlicher Fahrzeuge, Telefone und EDV-Geräte, die Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder die Aufnahme in Geburtstagslisten).

Abweichend von den Regelungen der Datenschutzgrundverordnung bedarf eine Einwilligung im Arbeitsverhältnis der Schriftform. Die Beschäftigten müssen ihre Einwilligung „in informierter Weise“ erteilen und daher über den Umfang unterrichtet werden. Dies umfasst auch eine Belehrung über den Zweck der

Datenverarbeitung sowie über die jederzeitige Widerrufsmöglichkeit. Allerdings kann der Widerruf der Einwilligung die Rechtmäßigkeit der Verarbeitung nicht rückwirkend beseitigen. Über diesen Umstand sind die Beschäftigten ebenso zu informieren. Siehe hierzu das Kurzpapier Nr. 14 der Datenschutzkonferenz, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf.

4. Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten sind 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.

Im Beschäftigungskontext ist die Verarbeitung solcher sensiblen Daten mittels Einwilligung möglich, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht. Aber auch ohne Einwilligung der betroffenen Person ist die Datenverarbeitung möglich, wenn hierzu in einer Kollektivvereinbarung (Tarifvertrag, Betriebs- oder Dienstvereinbarung) eine entsprechende Regelung enthalten ist oder wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist. So finden sich etwa in den Sozialgesetzbüchern (SGB) Regelungen zur Verarbeitung von sensiblen Daten. Im Rahmen einer erforderlichen Datenverarbeitung zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes muss darüber hinaus eine Interessenabwägung stattfinden und es darf kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse der Beschäftigten an dem Ausschluss der Verarbeitung überwiegt. Eine Kollektivvereinbarung muss diese Vorgaben gleichermaßen beachten, da sie das Schutzniveau der DSGVO nicht absenken darf.

III. Belehrungs-, Informations- und Auskunftspflichten

Einerseits ist wichtig, die Beschäftigten über die Verarbeitung ihrer eigenen Daten zu informieren, andererseits muss ebenso eine Sensibilisierung sowie Belehrung der Beschäftigten hinsichtlich eines datenschutzgerechten Umgang mit Kundendaten erfolgen. So kann gemäß einer Gerichtsentscheidung eine fristlose Kündigung zulässig sein, wenn ein Arbeitnehmer unrechtmäßig auf Kundendaten (Name und Kontodaten) zugreift. Dies gilt sogar dann, wenn der Arbeitnehmer sich darauf beruft, dass er lediglich eine Sicherheitslücke im System des Kunden aufdecken und davor warnen wollte. (Siehe hierzu Arbeitsgericht Siegburg, Urteil vom 22.11.2018, 5 Ca 1305/18, abrufbar unter http://www.justiz.nrw.de/nrwe/arbgs/koeln/arbg_siegburg/j2018/5_Ca_1305_18_Urteil_20181122.html)

Sowohl im Sinne des Arbeitgebers als auch der Beschäftigten empfehlen sich daher Schulungen der zum Datenschutz, um Datenmissbrauch zu verhindern.

1. Verpflichtung auf Geheimhaltung

Beschäftigte verarbeiten sowohl personenbezogene Daten anderer Beschäftigter als auch von Kunden, Dienstleistern, etc. (z.B. Anlegen von Adressverzeichnissen, Verarbeitung von Personaldaten, Versenden von Mails, Datenverarbeitung im Rahmen der Finanzbuchhaltung). In der Datenschutzgrundverordnung ist

jedoch keine Vorgabe dahingehend enthalten, eine Verpflichtung der Beschäftigten auf das Datengeheimnis einzuholen. Allerdings bestehen Dokumentationspflichten des Unternehmens. Sie müssen die Rechtmäßigkeit der Datenverarbeitung nachweisen können. Somit empfiehlt sich auch unter der Datenschutzgrundverordnung, die Beschäftigten auf das Datengeheimnis zu verpflichten. Die Aufsichtsbehörden haben hierzu eine Hilfestellung veröffentlicht: *„Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO“*, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf

Zu beachten ist:

Zur Verpflichtung gehört nach Auffassung der Datenschutzbehörden auch eine Belehrung über die sich ergebenden Pflichten. Mitarbeiter dürfen Daten zwar ausschließlich auf Weisung des Verantwortlichen verarbeiten, aber nicht alles kann detailliert in Arbeitsanweisungen geregelt werden, so dass eine Mitarbeiterschulung von besonderer Wichtigkeit ist. Die Beschäftigten sollten nach Auffassung der Aufsichtsbehörden somit -möglichst anhand typischer Fälle – darüber informiert werden, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen („Was sind personenbezogene Daten? Was umfasst eine rechtmäßige Datenverarbeitung? Welche Informationen dürfen gespeichert werden? Unter welchen Voraussetzungen dürfen Daten kopiert und weitergegeben werden? Welche Vorgaben sollten bei der Passworterstellung berücksichtigt werden?“). Dies beinhaltet eine laufende Sensibilisierung!

2. Informationspflichten gegenüber den Beschäftigten

Der Arbeitgeber muss die Betroffenenrechte der Datenschutzgrundverordnung sicherstellen. Hierzu zählen unter anderem Informationspflichten darüber, welche Daten zu welchem Zweck verarbeitet werden und wer Empfänger dieser Daten ist. Regelmäßig werden in Beschäftigungsverhältnissen Daten wie Name, Anschrift, Bankverbindung, Geburtsdatum, Steuerklasse, Zeugnisse, aber auch Arbeitszeiten, Gehaltsdaten, Kranken- oder Urlaubszeiten verarbeitet. Diesbezüglich muss eine Information darüber erfolgen, welche Daten des Beschäftigten zur Durchführung des Beschäftigtenverhältnisses erforderlich sind und verarbeitet werden, etwa für Zwecke der Lohnbuchhaltung, Entgeltauszahlung, aber auch im Rahmen der computergestützten Datenverarbeitung für die sichere Systemverwaltung. Die Informationspflicht umfasst gleichermaßen die Benennung eventueller Empfänger der Daten, z.B. Krankenversicherung oder sonstige Sozialversicherungsträger oder Finanzämter oder Rechtsanwälte im Falle von Rechtsstreitigkeiten, die das Arbeitsverhältnis betreffen.

Diese Daten sind im Übrigen identisch mit den Daten, die ein Arbeitgeber im Verzeichnis für Verarbeitungstätigkeiten aufzuführen hat.

3. Auskunftspflichten gegenüber den Beschäftigten

Das Auskunftsrecht zählt ebenso zu den Betroffenenrechten. Gemäß den Regelungen der DSGVO muss der Verantwortliche sogar eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen. Allerdings ist die Reichweite nicht geregelt und unklar: Können Beschäftigte daher die Aushändigung einer Kopie aller verfügbaren verarbeiteten personenbezogenen Daten, inklusive des gesamten E-Mailverkehrs verlangen? Diese Frage bzw. der Umfang der Auskunftspflicht wird von der Rechtsprechung derzeit uneinheitlich bewertet. So kann das Begehren auf Herausgabe des E-Mail-Verkehrs unverhältnismäßig sein, insbesondere wenn aufgrund der Insolvenz eines Arbeitgebers die

Wiederherstellung der Daten mit hohen Kosten verbunden ist (Landgericht Heidelberg, Urteil vom 06.02.2020, Az. 4 O 6/19). Andere Gerichte legen den Auskunftsanspruch dagegen sehr weit aus (z.B. Oberlandesgericht Köln, Urteil vom 26.07.2019, Az. 20 U 75/18, abrufbar unter https://www.iww.de/quellenmaterial/id/211714. Das OLG Köln hatte darüber zu entscheiden, inwieweit Gesprächsnotizen und Telefonvermerke ebenso von einem Auskunftsanspruch umfasst sein können). Für die Praxis gilt aus diesem Grunde, dass der Umfang dieses Rechts derzeit einer Einzelfallprüfung unterliegt.

Den Beschäftigten kann im Übrigen ein Schadensersatzanspruch zustehen, wenn der Arbeitgeber das Auskunftsrecht verletzt (siehe hierzu Arbeitsgericht Düsseldorf, Urteil vom 05.03.2020, Az. 9 Ca 6557/18, abrufbar unter https://www.justiz.nrw.de/nrwe/arbgs/duesseldorf/arbg_duesseldorf/j2020/9_Ca_6557_18_Urteil_20200305.html). Wird eine Auskunft nicht oder nicht vollständig erteilt, ist dies zum einen bußgeldbewehrt (Artikel 83 Abs. 5 b) DSGVO), zum anderen kann ein Anspruch auf Ersatz eines immateriellen Schaden zustehen. Im vorliegenden Fall hatte das Gericht den Arbeitgeber verurteilt, dem Beschäftigten einen Betrag in Höhe von 5000 EURO zu zahlen. Außerdem musste er Auskunft darüber erteilen, für welche Zwecke und Kategorien die personenbezogenen Daten des Beschäftigten verarbeitet werden.

IV. Videoüberwachung in der betrieblichen Praxis

1. Heimliche Videoüberwachung

Die Durchführung einer heimlichen Videoüberwachung von Beschäftigten ist nach der bisherigen Rechtsprechung des Bundesarbeitsgerichts nur im absoluten Ausnahmefall als letztes Mittel zulässig, wenn ein konkreter Verdacht einer strafbaren Handlung oder einer anderen schwerwiegenden Verfehlung besteht. Der Grund dafür ist, dass die Überwachung einen Eingriff in das allgemeine Persönlichkeitsrecht der Beschäftigten darstellt. Zwar kann sich auch ein Arbeitgeber auf grundrechtlich geschützte Positionen berufen (Eigentumsrecht und Berufsausübungsfreiheit). Aber insgesamt muss eine Interessenabwägung stattfinden.

Wird seitens des Arbeitgebers in unzulässiger Weise eine Videoüberwachung vorgenommen, dürfen die auf diese Weise gewonnenen Beweise nicht einem Gerichtsprozess gegen den Mitarbeiter verwendet werden.

Zu beachten ist:
Derzeit ist umstritten, ob eine heimliche Videoüberwachung unter der Datenschutzgrundverordnung erfolgen darf. Bereits unter der alten Rechtslage konnte die heimliche Videoüberwachung aufgrund der überwiegenden Interessen der Betroffenen nur in Ausnahmefällen in Betracht kommen. Argumente, welche dagegen sprechen, sind das in der DSGVO verankerte Transparenzgebot sowie die fehlende gesetzliche Legitimationsgrundlage, da die heimliche Videoüberwachung im BDSG nicht ausdrücklich genannt wird.Teilweise wird empfohlen, in solchen Fällen die Betriebsvereinbarung als Rechtsgrundlage für eine Videoüberwachung explizit festzulegen. In diesem Falle müsste jedoch zusätzlich geprüft werden, inwieweit die (heimliche) Videoüberwachung auf berechtigte Interessen gestützt werden kann. Alles in allem ist hiervon zurückhaltend Gebrauch zu machen, da sich diesbezüglich bislang noch keine einheitliche Meinung herausgebildet hat! So ist zu berücksichtigen, dass umstritten ist, inwieweit bei der Verarbeitung von Beschäftigtendaten überhaupt auf „berechtigte Interessen des Arbeitgebers“ zurückgegriffen werden darf. Der Deutsche Gewerkschaftsbund (DGB) und seine Mitgliedsgewerkschaften empfehlen insgesamt , in Dienst- und Betriebsvereinbarungen die Regelung aufzunehmen, dass heimliche Videoüberwachungen generell unzulässig sind.

2. Offene Videoüberwachung

Nach der Rechtsprechung des Bundesarbeitsgerichts kann auch eine *offene* Videoüberwachung nur in Ausnahmefällen in Betracht kommen. Mitentscheidend ist insbesondere die Intensität des Eingriffs für die Beschäftigten, die von den Bildaufnahmen erfasst sind, und ob die Maßnahme erforderlich ist oder der Zweck auch im Wege einer weniger einschneidenden Maßnahme erreicht werden kann. Zu prüfen ist, ob die Beschäftigten einem ständigen Überwachungsdruck ausgesetzt sind und damit in schwerwiegender Weise in das allgemeine Persönlichkeitsrecht eingegriffen wird und dadurch ein "Anpassungsdruck" erzeugt werden kann.

Zu beachten ist:
Die Intimsphäre muss unter allen Umständen unangetastet bleiben! In Umkleidekabinen oder Sanitärbereichen darf keine Videoüberwachung erfolgen. Abgeschlossene Schränke oder Schubladen gehören zwar nicht zur Intimsphäre, dürfen jedoch allenfalls im Beisein der Beschäftigten geöffnet werden.

3. Formale Anforderungen einer Videoüberwachung:

- **Verzeichnis von Verarbeitungstätigkeiten**

Grundsätzlich ist beim Einsatz von Überwachungssystemen (die natürliche Personen, wie beispielsweise Beschäftigte, betreffen) zu berücksichtigen, dass diese Form der Datenverarbeitung in einem so genannten **Verzeichnis von Verarbeitungstätigkeiten** aufzuführen ist, unter anderem auch unter Benennung von Löschungsfristen. Ein Muster für ein solches Verzeichnis ist unter https://www.datenschutzkonferenz-online.de/media/ah/201802_ah_muster_verantwortliche.pdf abrufbar, Musterbeispiele für kleine Unternehmen stellt das Bayerische Landesamt für Datenschutzaufsicht zur Verfügung (https://www.lda.bayern.de/de/kleine-unternehmen.html). Wichtig ist, dass die Bildaufnahmen stets nur solange verarbeitet werden dürfen, wie dies für die Erreichung des Zwecks erforderlich ist. Im Verzeichnis von Verarbeitungstätigkeiten sind daher auch der Zweck der Bildaufnahmen sowie Löschungsfristen zu definieren ("Wozu

werden die Aufnahmen benötigt"). Die Aufsichtsbehörden gehen davon aus, dass grundsätzlich nach 48 Stunden eine Löschung erfolgen sollte. Allerdings hat das Bundesarbeitsgericht bezüglich der Speicherdauer von Bildsequenzen, die ein strafrechtlich relevantes Verhalten der Beschäftigten zeigen, im Rahmen einer zulässigen offenen Videoüberwachung entschieden, dass die Auswertung des Videos nicht durch bloßen Zeitablauf unverhältnismäßig wird, solange die Ahndung der Pflichtverletzung durch den Arbeitgeber arbeitsrechtlich möglich ist. Dieses Urteil ist auf Kritik gestoßen, vor allem da die gerichtlichen Vorinstanzen entschieden hatten, dass aufgrund der nicht unverzüglichen Löschung des Videos ein Beweisverwertungsverbot vorliegt. (Siehe hierzu Bundesarbeitsgericht, Urteil vom 23.8.2018, 2 AZR 133/18, abrufbar unter https://juris.bundesarbeitsgericht.de/cgi-bin/rechtsprechung/document.py?Gericht=bag&Art=pm&Datum=2018&anz=40&pos=0&nr=21127&linked=urt).

- **Datenschutz-Folgenabschätzung**

Gerade beim Einsatz eines Videoüberwachungsgerätes ist zu prüfen, ob ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen (z.B. Beschäftigte) vorliegen könnte. In diesem Falle ist eine so genannte **Datenschutz-Folgenabschätzung** durchzuführen. Unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf ist seitens der Datenschutzaufsichtsbehörden eine entsprechende Orientierungshilfe für die Durchführung einer Datenschutz-Folgenabschätzung veröffentlicht worden.

- **Datenschutz durch Technik**

Gemäß der Datenschutzgrundverordnung muss außerdem der Grundsatz **"Datenschutz durch Technik"** beachtet werden. Dies bedeutet, dass die Unternehmen, die die Kameratechnik verwenden, bereits bei der Anschaffung der Technik die Datenschutzfreundlichkeit des Geräts überprüfen sollten. So verweisen die Aufsichtsbehörden darauf, bei der Beschaffung der Videotechnik auf den „eingebauten Datenschutz“ zu achten und empfehlen, dass nicht benötigte Funktionalitäten (z. B. freie Schwenkbarkeit, umfassende Überwachung per Dome-Kamera, Zoomfähigkeit, Funkübertragung, Internetveröffentlichung, Audioaufnahme) von der beschafften Technik nicht unterstützt oder zumindest bei der Inbetriebnahme deaktiviert werden sollten. Die Prüfung der Datenschutzfreundlichkeit bezieht sich auch darauf, inwieweit es möglich ist, Bereiche der Überwachung auszublenden, zu verpixeln oder bereits die Bildaufnahme so einzustellen, dass Personen optisch nicht identifizierbar sind. In Bezug auf den zuletzt genannten Punkt ist ergänzend anzumerken, dass eine Technik verwendet werden könnte, die Personen nicht erst im Nachhinein unkenntlich gemacht, sondern die von Beginn an ausschließlich Übersichtsaufnahmen erzeugt (siehe hierzu insgesamt das Kurzpapier Nr. 15 der Datenschutzkonferenz, abrufbar unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf).

- **Informationspflichten**

Grundsätzlich muss eine Videoüberwachung durch einen Hinweis auf diese Maßnahme kenntlich gemacht werden. Ein Beispiel für ein vorgelagertes Hinweisschild zur Erfüllung der Informationspflichten ist abrufbar unter https://www.lfd.niedersachsen.de/download/123756/Beispiel_fuer_ein_vorgelagertes_Hinweisschild.pdf.

Ein editierbares Informationsblatt findet sich unter https://www.lfd.niedersachsen.de/download/123756/Beispiel_fuer_ein_vorgelagertes_Hinweisschild.pdf und die Transparenzanforderungen

bei einer Videoüberwachung sind unter folgendem Link zusammengefasst: https://www.lfd.niedersachsen.de/download/123755/Transparenzanforderungen_und_Hinweisbeschilderung_bei_Videoueberwachung.pdf.

- **Zeitliche Beschränkung**

Im Verantwortungsbereich desjenigen, der Überwachungstechnik einsetzt, liegt außerdem die Prüfung, inwieweit eine solche zeitlich eingeschränkt werden kann. In Ihrem Kurzpapier zur Videoüberwachung (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf) verweisen die Aufsichtsbehörden darauf, dass in Zweifelfällen die zuständige Aufsichtsbehörde weiterhilft (siehe hierzu die Liste der Aufsichtsbehörden in Deutschland, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/die-aufsichtsbehorden-der-lander/) .

Zu beachten ist:

Die Zulässigkeit einer Videoüberwachung muss stets pro Betrieb und im Einzelfall bewertet werden. Im Übrigen ist zu beachten, dass die Einführung einer Videoüberwachung am Arbeitsplatz dem Mitbestimmungsrecht des Betriebsrats unterfällt, falls ein solcher vorhanden ist. In diesem Fall sollte die Durchführung und Auswertung der durch Videoüberwachung erzeugten Aufnahmen in einer Betriebsvereinbarung geregelt werden.

Für den Arbeitgeber ist **vor der Einführung der Videoüberwachungssysteme** erforderlich, den Betriebsrat einzuschalten. Dies ergibt sich aus dem Betriebsverfassungsgesetz.

In der Betriebsvereinbarung muss über die Videoüberwachung informiert werden.

Der Deutsche Gewerkschaftsbund (DGB) kritisiert, dass bei der Neufassung des § 26 BDSG die Videoüberwachung von Beschäftigten nicht spezifisch in einer gesetzlichen Bestimmung festgelegt wurde, obwohl diese in der Praxis von großer Bedeutung sei. Der DGB und seine Mitgliedsgewerkschaften empfehlen daher, bestimmte Punkte in Betriebs- und Dienstvereinbarungen ausdrücklich zu regeln, um die eingeschränkte Überwachung von Beschäftigten sicherzustellen. So sollte nach Auffassung des DGB etwa die Überwachung der öffentlich zugänglichen Teile des Betriebs oder der nicht öffentlich zugänglichen Teile des Betriebs, die nicht überwiegend der privaten Lebensgestaltung der Arbeitnehmer dienen (Foyer, Werkhallen, Eingangsbereich, Büro, etc.) nur aus Gründen der Sicherheit der Arbeitnehmer oder Betriebs zulässig sein, dabei jedoch nicht den Arbeitnehmer an seinem Arbeitsplatz umfassen (soweit nicht unumgänglich). Der DGB verweist ebenso darauf, dass das Merkmal „zur Wahrnehmung des Hausrechts“ in Bezug auf eine Videoüberwachung öffentlich zugänglicher Räume für europarechtswidrig eingestuft wird. Die heimliche Videoüberwachung soll nach Ansicht der Gewerkschaften in jedem Falle unzulässig sein.

V. Arbeiten im Homeoffice

Um das Arbeiten im heimischen Umfeld datenschutzgerecht zu ermöglichen, muss der Arbeitgeber die notwendigen technischen und organisatorischen Maßnahmen bereitstellen und den Beschäftigten in nachvollziehbarer Form erläutern. Die Maßnahmen beziehen sich einerseits auf den Schutz der personenbezogenen Daten, die im häuslichen Umfeld verarbeitet werden, aber andererseits ebenso auf die Wahrung der Intim- und Privatsphäre der Beschäftigten. So hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit beispielsweise kürzlich ausdrücklich vor dem Einsatz des Konferenztools Zoom

aufgrund der bekannt gewordenen Sicherheitsproblemen des Dienstes und der unverschlüsselten Speicherung des Inhalts der Gespräche auf den Servern des Anbieters gewarnt. Zu beachten ist in diesem Zusammenhang, dass das allgemeine Persönlichkeitsrecht auch das Recht am gesprochenen Wort schützt. Gespräche der Beschäftigten dürfen weder heimlich aufgenommen noch ohne ihre Einwilligung verwertet werden. Dies kann sogar strafrechtlich relevant sein.

Beschäftigte sollten beim Einsatz von Videokonferenzsystemen auch eigenverantwortlich und im eigenen Interesse berücksichtigen, dass Einblicke in ihr häusliches Umfeld möglich sind und etwa beim Teilen ihres Bildschirms darauf achten, ihren Mailaccount für die Zeit ihrer Teilnahme zu deaktivieren, da private Mails über Pop-Up-Fenster für die anderen Teilnehmer sichtbar werden können.

Im Falle der erlaubten dienstlichen Nutzung von privaten Endeinrichtungen der Beschäftigten kann der Arbeitgeber außerdem nicht verlangen, einen Messengerdienst zu installieren, der auf Kontaktdaten oder das Telefonverzeichnis zugreift. Allerdings ist der Einsatz privater Geräte im Rahmen dienstlicher Nutzung grundsätzlich als kritisch zu bewerten und Arbeitgeber dürfen in keinem Fall Zugriff auf die privaten Daten ihrer Beschäftigten nehmen. Die Beschäftigten sollten daher bereits im eigenen Interesse private und dienstliche Datenträger trennen und deutlich kennzeichnen. Dies gilt ebenso, wenn der Arbeitgeber im umgekehrten Falle den Beschäftigten die private Nutzung von dienstlichen Geräten erlaubt – hier sollten die Beschäftigten persönliche oder vertrauliche Dateiordner unmissverständlich benennen. Ein zusätzlicher Schutz der Beschäftigten besteht darin, dass ein Arbeitgeber niemals ohne Zustimmung des Betriebsrats ein System einführen darf, welches geeignet ist, das Verhalten der Beschäftigten, zu überwachen und zu protokollieren.

Die Beschäftigten sollten weiterhin mit dem Arbeitgeber klären, in welchen Grenzen sie berufliche Kontakte auf ihren privaten Geräten speichern dürfen. Insgesamt hängen Umfang und Beschränkungen stets vom Schutzbedarf der „dienstlichen" Daten ab. Wichtig ist, dass auf dem Endgerät der Beschäftigten keine App oder Messengerdienst installiert sind, die auf die dienstlichen Kontaktdaten zugreifen.

Mit Blick auf die personenbezogenen Daten von Kunden oder anderen Beschäftigten gilt, dass sensible personenbezogene Daten (z. B. Gesundheitsdaten oder Gewerkschaftszugehörigkeit) auch in einer Notsituation (wie der Corona-Pandemie) nur auf dienstlichen Geräten verarbeitet werden dürfen.

Allgemeine Hinweise zum Arbeiten im Homeoffice haben folgende Aufsichtsbehörden zur Verfügung gestellt:
Der Sächsische Datenschutzbeauftragter: https://www.saechsdsb.de/147-pandemie/607-datenschutz-bei-der-heimarbeit-bzw-im-home-office

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Home-office_bei_KMU.pdf

Das Bayerische Landesamt für Datenschutzaufsicht: https://www.lda.bayern.de/media/best_practise_homeoffice_baylda.pdf

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.pdf;jsessionid=C4EF821A5276F711605C4D21CDB98B43.1_cid344?__blob=publicationFile&v=26

Aktuell gibt es zur Bewältigung der Corona-Pandemie seitens der Aufsichtsbehörden **befristete Ausnahmeregelungen zum Einsatz von Videokonferenzen und Messengerdiensten**. Siehe hierzu:

Der Bayerische Landesbeauftragte für den Datenschutz: https://www.datenschutz-bayern.de/corona/sonderinfo.html

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Heimarbeit.pdf

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme-V1_1.pdf

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf

https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200525-PM-Empfehlungen_Durchfuehrung_Videokonferenzen.pdf

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg https://www.lda.brandenburg.de/sixcms/detail.php/bb1.c.662111.de

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Hinweise_zum_Datenschutz_im_Homeoffice.pdf

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat außerdem FAQ zum Thema Corona veröffentlicht: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/03/FAQ-Corona.pdf).

Ebenso hat der **Hamburgische Beauftragte für Datenschutz und Informationsfreiheit** Informationen zum Thema Corona unter https://datenschutz-hamburg.de/pages/corona-faq veröffentlicht.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen stellt Informationen zum Thema „Videokonferenzsysteme“ und „Messengerdienste“ bereit: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Schule_-Videokonferenzsysteme-und-Messenger-Dienste-waehrend-der-Corona-Pandemie/LDI-NRW---Videokonferenzsysteme-18_05_2020.pdf.

Allgemeine Fragen und Antworten zur Bewältigung der Corona-Pandemie und möglichen Kontrollrechten des Arbeitgebers hat außerdem die **Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)** in FAQ zusammengestellt, abrufbar unter https://www.gdd.de/datenschutz-und-corona/FAQ-Corona. Sie bezieht sich in Ausführungen auf die Fürsorgepflicht der Arbeitgeber, die diese nach den Regelungen des Arbeitsschutzgesetzes (ArbSchG) umsetzen müssen.

VI. Fallbeispiele

1.

Malermeister Kurt Leiste beschäftigt zwei Angestellte, für die er jeweils handschriftliche Ordner mit ihren Stammdaten angelegt hat. Auf einem Zettel notiert er, dass Hassan eine Woche wegen Schnupfen krankgeschrieben ist und Henriette schon wieder an einem Montag zu spät im Betrieb erscheint. Bei der Neu-Anstellung der Aushilfe Hubsi ergänzt er beim Anlegen des Personalordners handschriftlich die Konfession zu dessen Name und Anschrift.

Die Anwendbarkeit der Vorschriften der DSGVO und des BDSG setzt im Beschäftigtenverhältnis keine automatisierte bzw. IT-gestützte Verarbeitung von Personaldaten voraus. Die Papierform ist ausreichend (§ 26 Abs. 7 BDSG).

Die Verarbeitung besonderer Kategorien von Daten (z. B. Religionszugehörigkeit, Gesundheitsdaten) kann zur Erfüllung der Pflichten aus dem Arbeitsrecht oder des Sozialschutzes (SGB) erforderlich sein. In diesem Falle ist bei der Verarbeitung dieser sensiblen Daten keine Einwilligung der Beschäftigten erforderlich, es sei denn das Interesse des Beschäftigten an dem Ausschluss der Verarbeitung überwiegt. Zu berücksichtigen ist dabei, dass Angaben zur Religionszugehörigkeit **nur** für die Abführung von **Kirchensteuer** erhoben und genutzt werden dürfen. Bei einer längerfristigen Speicherung von Beschäftigtendaten, etwa beim Führen von Personalakten, gilt der Maßstab der Erforderlichkeit sowie der Verhältnismäßigkeit. Informationen zur Identität der Beschäftigten sind erforderlich (Name, Anschrift, Alter, Geschlecht, Familienstand, Schulabschluss und Ausbildung). Für die Beurteilung im gesamten ist wesentlich, ob die langfristig gespeicherten Daten die Persönlichkeitsrechte der Beschäftigten beeinträchtigen. **Eine Speicherung von Informationen zu konkreten Krankheitsgründen oder Notizen des Arbeitgebers über die Leistungen oder Nichtleistungen der Beschäftigten können einen Eingriff in das Persönlichkeitsrecht des Arbeitnehmers begründen**. Eine **Abmahnung** hingegen darf als Dokumentation eines Fehlverhaltens in der Personalakte geführt werden. Von besonderer Bedeutung ist es außerdem, den Zugriffschutz auf die gespeicherten Daten sicherzustellen. So gilt für ärztliche Gutachten, Gesundheitszeugnisse, etc., dass diese in verschlossenen Umschlägen zur Personalakte zu nehmen sind.

Ausblick: Aufgrund der Einführung einer digitalen Arbeitsunfähigkeitsbescheinigung entfällt zukünftig die Verpflichtung zur Vorlage einer Arbeitsunfähigkeitsbescheinigung, da der Arbeitgeber diese ab dem Jahre 2021 bei den Krankenkassen digital abrufen kann. Die Beschäftigten müssen jedoch nach wie vor ihre Arbeitsunfähigkeit dem Arbeitgeber melden und benötigen eine ärztliche Feststellung. Zurzeit müssen die Beschäftigten ihrem Arbeitgeber ab dem dritten Tag ihrer Arbeitsunfähigkeit eine Bescheinigung vorlegen.

2.

Die Auszubildende Ayse hat ihr Ausbildungsverhältnis bei der „Glücklich"-e.G. begonnen und erhält kurz darauf einen Brief von der „V.Traut"-Versicherung, welche dem Konzernverbund der „Glücklich"-e.G. angehört. Das Versicherungsunternehmen bietet ihr 30% Rabatt an, wenn sie eine private Unfallversicherung abschließt. Auf Nachfrage bei ihrem Chef, erhält Ayse die Auskunft, dass der

Betriebsrat der „Glücklich"-e.G. der Übermittlung von Name und Adresse an die „V.Traut"-Versicherung zugestimmt habe und außerdem aufgrund des Konzernverbundes die Daten im Unternehmen ausgetauscht werden dürfen.

Die datenschutzfreundliche Ayse hat dennoch Bedenken. Zu Recht?

Auszubildende fallen unter den Begriff der „Beschäftigten". Auch unter der Datenschutzgrundverordnung gibt es kein Konzernprivileg! Jedes rechtlich selbstständige Konzernunternehmen ist ebenso wie jedes andere Unternehmen „Dritter" im datenschutzrechtlichen Sinne. Daher ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung erlaubt. Die Datenschutzgrundverordnung führt zwar hierzu aus, dass innerhalb einer Unternehmensgruppe ein berechtigtes Interesse dahingehend bestehen kann, personenbezogene Daten für interne Verwaltungszwecke zu übermitteln. Diese sind hier jedoch auszuschließen, da es sich um Werbung handelt, die für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich ist. Dieses Ergebnis würde selbst dann gelten, wenn man zusätzlich das Vorliegen eines berechtigten Interesses des Arbeitgebers prüfen würde, da das Interesse der Beschäftigten an dem Ausschluss der Übermittlung für Werbezwecke überwiegt. Die Zustimmung des Betriebsrats ist mangels Zuständigkeit unwirksam und eine Betriebsvereinbarung nichtig, da bei Werbepost keine betrieblichen Interessen betroffen sind. Zudem muss der Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer schützen und fördern. Hier würde daher zusätzlich ein Eingriff in das Persönlichkeitsrecht der Beschäftigten vorliegen.

(Siehe hierzu Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage, S. 45)

3.
Ferdinand ist Arbeitgeber. Von Bewerbern lässt er einen umfassenden Fragebogen ausfüllen. Unter welchen Voraussetzungen darf Ferdinand Daten der Bewerberinnen und Bewerber erheben und verarbeiten?

Personenbezogene Daten einer Bewerberin oder eines Bewerbers dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Die Fragen des Bewerbungsbogens sind stets unter dem Aspekt stellen, ob diese für die Begründung des konkreten Beschäftigungsverhältnisses erforderlich sind.

4.
Darf der Ferdinand in dem Bewerbungsbogen die Frage stellen, ob eine Behinderung vorliegt?

Die Frage nach einer Schwerbehinderung stellt einen Eingriff in das allgemeine Persönlichkeitsrecht der Bewerberin oder des Bewerbers dar und verletzt damit das informationelle Selbstbestimmungsrecht. Diese Wertung ergibt sich auch aus dem Allgemeinen Gleichbehandlungsgesetz (AGG). Ziel dieses Gesetzes ist es, Benachteiligungen unter anderem aus Gründen einer Behinderung zu verhindern. Der Arbeitgeber darf danach pauschal keine Auskunft darüber verlangen, ob eine Behinderung vorliegt. Er könnte allenfalls fragen, ob die Bewerberin oder der Bewerber an gesundheitlichen, seelischen oder anderen Beeinträchtigungen leidet, durch die sie oder er für die Erfüllung der erwarteten arbeitsvertraglichen Pflichten ungeeignet ist, und zwar wenn dies gerade die wesentliche Voraussetzung für den konkreten

Arbeitsplatz darstellt. Die pauschale Frage nach Schwerbehinderung ist demnach unzulässig und würde eine unmittelbare Diskriminierung der Bewerberin oder des Bewerbers darstellen.

5.
Darf Ferdinand im Bewerbungsbogen nach Vorstrafen fragen?

Nach Vorstrafen darf die Bewerberin oder der Bewerber bei der Einstellung nur gefragt werden, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert. Ein Kassierer darf etwa nach Vermögensdelikten und eine LKW-Fahrerin nach Verkehrsdelikten gefragt werden. Vorstrafen, die im Bundeszentralregister bereits getilgt sind, müssen nicht angegeben werden. Auch die Vorlage eines polizeilichen Führungszeugnisses kann damit nicht pauschal verlangt werden, da darin sämtliche Vorstrafen erfasst sind.

6.
Darf Zahnarzt Zausel die Bewerberin Amelie, die sich um die Stelle als Arzthelferin bewirbt, die Frage nach einer möglichen Schwangerschaft stellen (aufgrund der Röntgenbelastung und zum Schutz des Kindes)?

Die Frage nach einer Schwangerschaft stellt einen Eingriff in das allgemeine Persönlichkeitsrecht der Bewerberin und verletzt damit das informationelle Selbstbestimmungsrecht. Diese Wertung ergibt sich auch aus dem Allgemeinen Gleichbehandlungsgesetz. Ziel dieses Gesetzes ist es, Benachteiligungen unter anderem aus Gründen des Geschlechts zu verhindern. Dies gilt ebenso, wenn der Arbeitgeber die Stelle aufgrund der Schwangerschaft (zunächst) aus gesundheitlichen Gründen und aufgrund mutterschutzrechtlicher Vorschriften nicht besetzen darf.

Insgesamt gilt:

Ein Arbeitgeber/Eine Arbeitgeberin kann einen Arbeitsvertrag anfechten, sofern ein Arbeitnehmer/eine Arbeitnehmerin bei der Einstellung gelogen hat, aber nur wenn Pflicht zur Wahrheit besteht. Insgesamt ist das Fragerecht im Rahmen von Bewerbungsgesprächen begrenzt. Arbeitgeber und Arbeitgeberinnen haben das Persönlichkeitsrecht der Beschäftigten zu beachten und dürfen nicht in deren Intimsphäre durch indiskrete Fragen eingreifen. Bei unzulässigen Fragen hat der Arbeitnehmer/die Arbeitnehmerin ein Recht auf Lüge. So sind Fragen zur Religionszugehörigkeit nur zulässig, soweit es sich um einen so genannten Tendenzbetrieb handelt, und die Frage nach einer Gewerkschaftszugehörigkeit ist grundsätzlich unzulässig. Unzulässig ist ebenso die Frage bezüglich der Familien- oder Heiratsplänen. Allerdings soll in besonderen Ausnahmefällen die Frage nach dem Familienstand zulässig sein, etwa bei unvorhersehbaren Einsätzen und ungewöhnlichen Zeiten und Alleinerziehenden. Sofern der Arbeitnehmer/die Arbeitnehmerin in der zukünftigen Stellung eine Vertrauensposition innehat, kann im Übrigen ein zulässiges Fragerecht hinsichtlich der Vermögensverhältnisse bestehen. Die Frage nach der bisherigen Vergütung ist unzulässig, sofern diese für die neue Stelle unerheblich ist (z.B. keine Aussage über Qualifikation enthält) und die Bewerberin/der Bewerber diese nicht als Mindestvergütung fordert.

7.
Dürfen Arbeitgeber/Arbeitgeberinnen eine Interessentendatenbank erstellen? – Wie lange dürfen sie diese Daten speichern?

Daten von Bewerbern und Bewerberinnen sollten nicht länger als vier Monate gespeichert und danach gelöscht werden. Sofern Arbeitgeber oder Arbeitgeberinnen für zukünftige Stellenbesetzungen Interesse an einer längerfristigen Speicherung haben, muss die freiwillige und informierte Einwilligung der Bewerber und Bewerberinnen eingeholt werden. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg 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 (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigtendatenschutz.pdf). Grundsätzlich gilt, dass ein abgelehnter Bewerber/eine abgelehnte Bewerberin nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) zwei Monate Zeit hat, bei einem Verstoß gegen das Benachteiligungsverbot im Rahmen des Auswahlverfahrens einen Schadensersatzanspruch geltend zu machen. Daher können Bewerbungsunterlagen frühestens nach zwei Monaten gelöscht werden, damit Arbeitgeber und Arbeitgeberinnen die Möglichkeit haben, sich gegen mögliche Ansprüche zu verteidigen. In der Praxis ist die zulässige Höchstspeicherfrist von Bewerberunterlagen noch nicht abschließend geklärt. Aus Gründen der Verhältnismäßigkeit ist eine längere Speicherdauer als vier Monate jedoch nicht erforderlich.

8.
Arbeitgeberin Constanze freut sich über die Unterstützung moderner Kommunikationsmittel. Dies spart Zeit und Kosten.

a) Darf sie ein Bewerbungsgespräch via Skype durchführen?

In der beruflichen Praxis wird die Zulässigkeit unterschiedlich beurteilt und eine freiwillige Einwilligung unter Beachtung der Informationspflichten bejaht.

Zu beachten ist allerdings die Auffassung der Aufsichtsbehörden: Berliner Beauftragte für Datenschutz und Informationsfreiheit, die im Rahmen der Erforderlichkeitsprüfung auf die schutzwürdigen Belange der Bewerberinnen und Bewerber verweist (Tätigkeitsbericht 2016, S. 116, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2016-Web.pdf). Sie weist darauf hin, dass in objektiver Hinsicht der Einsatz von Skype regelmäßig nicht geboten sei. Sofern die Betroffenen jedoch selbst die Nutzung von Skype wünschen, sei grundsätzlich von einer Freiwilligkeit auszugehen sein. Allerdings müssten die Betroffenen über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten sowie über die Empfänger der Daten aufgeklärt werden.

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat insgesamt empfohlen, von der Nutzung von Skype abzusehen und darauf verwiesen, dass nach den Nutzungsbedingungen von Skype Chat-Protokolle auf den Servern von Microsoft in den USA bis zu 90 Tage zwischengespeichert werden. Wenn der Bewerber/die Bewerberin allerdings die Skype-Nutzung selbst wünscht, so ist eine freiwillige Einwilligung zu unterstellen. Der Bewerber/die Bewerberin ist dennoch über die Datenverarbeitung durch Skype und Microsoft zu informieren.

Die Aufsichtsbehörden haben zwar für die Zeit der Corona-Pandemie befristete Regelungen zum Einsatz von Messenger- und Videokonferenzsystemen veröffentlicht. Dennoch gilt, dass nach wie vor der Datenschutz beachtet werden muss. Es sollte daher vorrangig geprüft werden, ob alternativ eine Telefonkonferenz durchgeführt werden kann, wenn bei mehr als zwei Beteiligten keine Ende-zu-Ende-Verschlüsselung der Kommunikation möglich ist. Ansonsten sollten Anbieter von Videokonferenzsystemen mit Sitz in der EU, EFTA oder Schweiz gewählt werden, wenn innerhalb der Onlinesitzung sensible Daten besprochen werden sollen.

b) Darf Constanze als Arbeitgeberin ein Videointerview anstatt eines persönlichen Bewerbungsgesprächs durchführen?

Hier verweisen die Berliner Beauftragte für Datenschutz und Informationsfreiheit sowie **Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen** in ihren Tätigkeitsberichten darauf, dass durch den Einsatz von Videotechnik bzw. der Aufzeichnung des Gesprächs ein Eingriff in das informationelle Selbstbestimmungsrecht vorliegt. Begründet wird dies mit einer wesentlichen intensiveren Auswertungsmöglichkeit des Verhaltens und der Persönlichkeit der Bewerber und Bewerberinnen.

Berliner Beauftragte für Datenschutz und Informationsfreiheit (Tätigkeitsbericht 2016, S. 117):

„Die zusätzliche Erhebung und Nutzung von Bild- und Tonaufzeichnungen der Bewerberinnen und Bewerber stellt einen wesentlich intensiveren Eingriff in deren informationelles Selbstbestimmungsrecht dar als die übliche Beantwortung von Fragebögen o. Ä. Eine videogestützte Befragung bzw. eine zeitversetzte Auswertung der Videointerviews für eine Bewerberauswahl ist in keiner Hinsicht notwendig. Derartige Videointerviews sind rechtswidrig."

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (Tätigkeitsbericht 2017, S. 52/53):

„Das geschilderte Verfahren ist datenschutzrechtlich unzulässig. Derartige Videointerviews mit zeitversetzter Auswertung greifen erheblich stärker in das Recht auf informationelle Selbstbestimmung der Bewerberinnen und Bewerber ein als herkömmliche Auswahlgespräche. Im Unterschied zu flüchtigen, weil nicht reproduzierbaren Wahrnehmungen in einem Gespräch ermöglicht die Aufzeichnung von Ton und Bild eine detailliertere und intensivere Auswertung auch des nonverbalen Verhaltens (etwa Mimik, Gestik, Tonfall)."

c) Darf Arbeitgeberin Constanze die Nutzung von WhatsApp für die betriebliche Kommunikation regeln?

Problematisch bei der Verwendung von WhatsApp sind die Nutzungsbestimmungen dieses Dienstes.

Richtlinie WhatsApp:

„Im Einklang mit geltenden Gesetzen stellst du uns regelmäßig die Telefonnummern in deinem Mobiltelefon-Adressbuch zur Verfügung, darunter sowohl die Nummern von Nutzern unserer Dienste als auch die von deinen sonstigen Kontakten.“

Zu beachten ist jedoch, dass regelmäßig von den im Adressbuch aufgelisteten Personen keine Erlaubnis zur Weitergabe ihrer Telefonnummer an WhatsApp erteilt wurde, aber diese Daten dennoch übertragen und auf Servern in den USA gespeichert werden. WhatsApp erhält hierbei Kenntnis von den Metadaten (Zeitpunkt und Dauer der Kommunikation, IP-Adresse, Geräte-ID, etc.), die Rückschlüsse auf die Beteiligten zulassen und Profilerstellung zulassen. Zudem ist die dauerhafte Verschlüsselung der Text- und Bilddaten fraglich.
Seitens der Aufsichtsbehörden wird regelmäßig betont, dass der Einsatz von WhatsApp durch Unternehmen zur betrieblichen Kommunikation gegen die Datenschutz-Grundverordnung (DS-GVO) verstößt. Eine datenschutzkonforme Nutzung von WhatsApp ohne Übertragung von Telefonnummern ist also nur bei dauerhafter Deaktivierung des Zugriffs auf die Kontakte direkt nach der Installation möglich.

Empfehlung: Auf die Nutzung von WhatsApp sollte im betrieblichen Kontext verzichtet werden. Auch wenn die private Nutzung nicht unter das Datenschutzrecht fällt und damit nicht sanktioniert wird, ist grundsätzlich zu prüfen, inwieweit das Betriebssystem des Smartphones die Deaktivierung der Synchronisation der Kontaktdaten unterstützt

9.
Darf sich die Arbeitgeberin Zeynep im Internet (z.B. Suchmaschinen) Informationen über Bewerber und Bewerberinnen im Rahmen eines „Background-Checks“ einholen und frühere Arbeitgeber und Arbeitgeberinnen anrufen, um persönliche Erkundigen einzuholen?

Gemäß einer BITKOM-Pressemitteilung überprüfte bereits im Jahr 2015 jedes zweite Unternehmen Bewerberinnen und Bewerber in sozialen Netzwerken (BITKOM = Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.). Hierbei stehen nach Auskunft der BITKOM fachliche Qualifikationen und Äußerungen der Bewerberinnen und Bewerber im Vordergrund, wobei jeder siebte Bewerber bzw. Bewerberin nach dieser Prüfung bereits vorher aussortiert werde. Von Aufsichtsbehörden wird allerdings die Auffassung vertreten, dass Recherchen in sozialen Netzwerken wie facebook oder twitter aus datenschutzrechtlicher Sicht stets unzulässig sind, es sei denn es handelt sich um berufliche Netzwerken wie etwa XING oder LinkedIn.

Aufgrund des Grundrechts auf informationelle Selbstbestimmung sind die Daten außerdem grundsätzlich beim Bewerber zu erwerben. BewerberInnen sollen entscheiden können, welche Daten der neue Arbeitgeber über sie erfährt. Sollen bei einer früheren Arbeitgeberin Erkundigungen eingeholt werden, ist dies daher nur mit freiwilliger Einwilligung der Bewerberin oder des Bewerbers möglich und wenn diese zuvor darüber informiert wurden. In diesem Zusammenhang muss der Arbeitgeber/die Arbeitgeberin allerdings beachten, inwieweit eine *freiwillige* Erklärung im Arbeitsverhältnis tatsächlich umgesetzt werden kann.

Im Hinblick auf die Informationsbeschaffung durch allgemein zugängliche Suchmaschinen wird darüber hinaus die Auffassung vertreten, dass diese zulässig ist, wenn sie für die Einstellungsentscheidung erforderlich ist und ausschließlich Informationen betrifft, die vom Fragerecht umfasst sind. In diesem Falle muss

dieser Umstand dem Bewerber bzw. der Bewerberin jedoch spätestens innerhalb eines Monats nach Erlangung der personenbezogenen Daten mitgeteilt werden und ebenso eine Information über die Quellen und die Rechtsgrundlage der Verarbeitung erfolgen. Allerdings wird dies nicht einheitlich beurteilt, so dass sich eine gesetzliche Klarstellung empfehlen würde.

10.
Macht sich Arbeitgeber Hakim strafbar, sofern er die privaten und geschäftlichen Telefonate seiner Arbeitnehmer ohne deren Wissen mithört?

Strafrechtlich relevant ist lediglich das Aufnehmen des nicht-öffentlich gesprochenen Wortes oder die Zugänglichmachung an Dritte. Das reine Mithören ist strafrechtlich nicht relevant (zumindest nicht bei handelsüblichen bzw. gebräuchlichen Mithörvorrichtungen in privaten oder geschäftlichen Telefonanlagen). Zu berücksichtigen ist dennoch das Persönlichkeitsrecht der Beschäftigten: Das Recht am gesprochenen Wort ist geschützt und es liegt ein Eingriff in das Persönlichkeitsrecht der Beschäftigten vor, wenn der Arbeitgeber die Vertraulichkeit der Kommunikation verletzt. Dies gilt unabhängig davon, ob es sich um private oder geschäftliche Kommunikation handelt.

(Vgl. hierzu auch ausführlich Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage, S. 150)

11.
Arbeitgeber Ferdinand ist der Auffassung, dass er die Mails seiner Mitarbeiter und Mitarbeiterinnen jederzeit lesen darf, sofern es sich um betriebliche Kommunikation handelt. Die Beschäftigten Hakan und Charlotte haben Bedenken und weisen darauf hin, dass dies in einer Betriebsvereinbarung geregelt werden müsse.

Der bereitgestellte Mail-Account zählt zu den Betriebsmitteln, über die der Arbeitgeber entscheidet und die seinem Direktionsrecht unterliegen. Er kann daher die private Nutzung verbieten und bei dienstlicher Kommunikation jederzeit Einsicht verlangen bzw. sich diese zeigen lassen, sofern nicht die Korrespondenz mit betrieblichen Vertrauensstellen (z.B. Betriebsrat, Betriebsarzt) betroffen ist. Allerdings ist das Urteil des Europäischen Gerichtshofs für Menschenrechte vom 05.09.2017 (https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-177083%22]}) zu beachten. Der zugrundeliegende Fall bezieht sich auf Messenger-Nachrichten, deren Kontrolle –auch beim Verbot privater Nutzung – zwar möglich aber beschränkt ist. So müssen Beschäftigte über Ausmaß und Umfang der Kontrolle vorab informiert werden, so dass eine lückenlose Überwachung gegen das Persönlichkeitsrecht der Beschäftigten verstößt. Dies betrifft im Übrigen ebenso die derzeit bestehende Streitfrage, inwieweit unter der DSGVO aufgrund des Transparenzgrundsatzes eine heimliche Überwachung von Beschäftigten in Betracht kommen kann. In der Praxis ist außerdem zu berücksichtigen, dass Mails, selbst wenn diese aus dienstlichem Grund verfasst sind, mit dem formalen Schriftverkehr nicht gleichgesetzt werden können. Die Kommunikation per Mail ist regelmäßig weniger formal. Insgesamt darf der Inhalt von E-Mails vom Arbeitgeber nicht weiter zur Kenntnis genommen werden, wenn diese erkennbar privat sind. Eine andere Bewertung kann sich allenfalls im Rahmen von zulässigen Missbrauchskontrollen ergeben.

12.
Arbeitgeber Ferdinand führt bei sämtlichen Einstellungen routinemäßig einen Drogentest durch. Er verweist darauf, dass er keine „Straftäter" in seinem Betrieb beschäftigen wolle.

Die Durchführung eines Drogentests muss für die Besetzung der konkreten Stelle erforderlich sein. Im Hinblick auf Drogentests stellt der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg klar, dass der Test darauf gerichtet sein muss, eine Alkohol-oder Drogenabhängigkeit nachzuweisen und es dürfe nicht lediglich darum gehen, den Alkohol-oder Drogenkonsum zu ermitteln. Arbeitsplatzrelevantes Verhalten liege allerdings nur vor, wenn die Beschäftigten durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte des Unternehmens gefährden könnte (https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigtendatenschutz.pdf).

(Vgl. hierzu auch Gola/Reif, Praxisfälle Datenschutzrecht, 2. Auflage, S. 130).

13.
Der misstrauische Arbeitgeber Konrad Controletti möchte seine Außendiensmitarbeiterinnen und Außendienstmitarbeiter besser im Blick haben. Daher lässt er sämtliche Dienstfahrzeuge mit einem Ortungssystem ausstatten.

Die umfassende und anlasslose Überwachung von Arbeitnehmerinnen und Arbeitnehmern ist unzulässig.

14.
Ändert sich etwas, wenn Konrad Controletti die Fahrzeuge vor Diebstahl schützen möchte und das Ortungssystem dazu dienen soll, Mitarbeiter- und Fahrzeugeinsätze besser zu koordinieren?

Die Verarbeitung von GPS-Daten muss für die Durchführung des Beschäftigungsverhältnisses erforderlich sein. Es ist außerdem zu beachten, dass beim Einsatz von Ortungssystemen, wie z.B. GPS, Informationspflichten gegenüber den Beschäftigten zu erfüllen sind. Die Verwendung eines solches Systems muss transparent sein. Hierzu wird ebenso vertreten, dass auch der Anruf auf dem Mobiltelefon der Beschäftigten ausreichend sein kann, um den Aufenthaltsort zu ermitteln: So vertritt das Verwaltungsgericht Lüneburg die Auffassung, dass Ortungssysteme für präventiven Diebstahlsschutz ungeeignet sind. So reiche für das Wiederauffinden entwendeter Firmenfahrzeuge die anlassbezogene Erhebung im Falle eines festgestellten Fahrzeugverlustes aus, so dass eine ständige Erfassung der Fahrzeugposition nicht erforderlich sei (VG Lüneburg vom 19.03.2019, abrufbar unter http://www.rechtsprechung.niedersachsen.juris.de/jportal/portal/page/bsndprod.psml?doc.id=MWRE190000986&st=null&doctyp=juris-r&showdoccase=1&paramfromHL=true#focuspoint).

In Bezug auf die Koordination der Arbeitseinsätze beurteilt das VG Lüneburg die Erforderlichkeit für Zwecke des Beschäftigungsverhältnisses im Hinblick auf den Betriebsablauf eines Gebäudereinigungsunternehmen und kommt zu dem Ergebnis, dass die Speicherung von während der Arbeitszeiten anfallenden Daten über das Ortungssystem zum Zwecke der Planung von Touren oder der Koordination von Mitarbeitern und Fahrzeugen ebenfalls nicht erforderlich ist. So sei die Tourenplanung zukunftsorientiert und Informationen über aktuelle und vergangene Standorte der Firmenfahrzeuge damit planungsunerheblich.

Die ständige Erfassung von Standort-, Bewegungs- und Zeitdaten der Firmenfahrzeuge sei nicht erforderlich und die Erreichbarkeit mittels Mobiltelefon könne ebenso als milderes Mittel ausreichend sein. Eine andere Beurteilung kann sich nach Auffassung des Gerichts jedoch ggf. im Transport- und Beförderungsgewerbe ergeben (siehe hierzu insgesamt VG Lüneburg aaO).

15.
Rinku ist in der Personalabteilung eines großen Getränkefachhandels beschäftigt und hat Zugriff auf die unterschiedlichen Beschäftigtendaten. Darf seine Arbeitgeberin seine Zugriffe auf die Beschäftigtendatenbank protokollieren? Rinku hat die Befürchtung, dass seine Arbeitgeberin nachprüft, welche Zeitdauer er für die einzelne Fallbearbeitung benötigt und unterstellen könnte, dass er nicht effizient arbeitet.

Der Umgang mit Protokolldaten kann in der Praxis eine Herausforderung darstellen, da einerseits die Dokumentation sowohl aus revisionsrechtlichen als auch aus datenschutzrechtlichen Gründen erforderlich sein kann, andererseits aber die Gefahr einer Leistungs- und Verhaltenskontrolle von Beschäftigten besteht. Zu berücksichtigen ist, dass jeder Verantwortliche, z.B. ein Arbeitgeber, die datenschutzkonforme Verarbeitung nachweisen muss. So kann damit der Nachweis der Umsetzung der gesetzlichen Datenschutzanforderungen im Sinne einer technisch-organisatorischen Maßnahme verbunden sein. Insbesondere wenn es sich um Zugriffsmöglichkeiten der Beschäftigten auf sensible Daten von Kunden oder Kollegen handelt, kann ein Bedarf an einer Protokollierung bestehen - beispielsweise auch zur Dokumentation, dass keine unberechtigten Zugriffe auf personenbezogene Daten erfolgen. Die Protokollierung ist also eine wichtige Maßnahme, um später überhaupt beurteilen zu können, ob die (bereits zurückliegende) Datenverarbeitung aus datenschutzrechtlicher Sicht rechtmäßig war. Allerdings müssen im Vorfeld die Zwecke der Auswertung detailliert beschrieben werden (etwa der durch konkrete Tatsachen begründete Verdacht einer Straftat). Ebenso muss der Zugriff auf die Protokolldaten datenschutzrechtlichen Anforderungen genügen und erfordert ein detailliertes Berechtigungskonzept. Dies bedeutet, dass die Zwecke der Auswertung klar definiert werden müssen und die Auswertung selbst nur von Personen vorgenommen werden darf, die hierzu befugt sind. Es müssen außerdem Löschungsfristen für die aufgezeichneten Daten bzw. die Protokolldaten definiert sein. Gegebenenfalls müssen die Protokolldaten nach dem Stand der Technik verschlüsselt werden. Die Definition des Zwecks darf nicht allgemein und pauschal, etwa zum Zwecke der „IT-Sicherheit“ definiert sein. Soll eine Auswertung erfolgen, muss vielmehr ein konkreter Verdacht vorliegen. Eine Überwachung ins Blaue hinein ist unzulässig. Es ist sicherzustellen, dass eine Verhaltens- und Leistungskontrolle ausgeschlossen ist. Daher können (im ersten Schritt) ebenso nicht-personenbezogene Auswertungen und Stichproben ausreichend sein. Außerdem ist der Betriebsrat einzubinden – vorausgesetzt, dass ein solcher im Betrieb vorhanden ist.

16.
Wie ist die rechtliche Situation zu bewerten, wenn Konrad Controletti ein elektronische Zeiterfassung mittels Fingerprint einführt? Hakan und Charlotte verweisen wiederum auf eine fehlende Kollektivvereinbarung und eine freiwillige Einwilligung der Beschäftigten.

Bei einem Fingerabdruck handelt es sich biometrische Daten gemäß Artikel 9 Abs. 1 DSGVO bzw. besondere Kategorien personenbezogener Daten gemäß § 26 Abs. 3 BDSG, deren Verarbeitung grundsätzlich verboten ist, es sei denn es liegt eine gesetzlich geregelte Ausnahme vor, wie etwa eine (freiwillige) Einwilligung. Zu berücksichtigen ist, dass die Verarbeitung eines Fingerabdrucks die Privatsphäre

und damit das Recht auf informationelle Selbstbestimmung im besonderen Maße verletzen kann und somit auch besonders hohe Anforderungen an die Rechtmäßigkeit zu stellen sind. Sofern keine Einwilligung vorliegt, muss die Verarbeitung erforderlich sein, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben kann. Im Rahmen der damit verbundenen Verhältnismäßigkeitsprüfung muss der Arbeitgeber daher prüfen, ob dass das schutzwürdige Interesse der betroffenen Personen (der Beschäftigten) an dem Ausschluss der Verarbeitung überwiegt. Damit ist auch die kritische Prüfung verbunden, ob im betrieblichen Alltag ein anderes, gleich wirksames Verfahren eingeführt werden kann, das weniger gravierend in das Persönlichkeitsrecht eingreift. Dies ist stets Frage des Einzelfalls und muss vom Arbeitgeber entsprechend dargelegt werden. Dazu kann die Prüfung und Begründung gehören, aus welchen Gründen kein manuelles Zeiterfassungsverfahren in Betracht kommt oder ob besondere Gründe vorliegen, die ein Fingerprintverfahren aus Missbrauchsgesichtspunkten erforderlich machen. Dabei muss in die Abwägung ebenso einbezogen werden, welchen Zweck das biometrische Verfahren verfolgt. Hierzu wird die Auffassung vertreten, dass biometrische Daten zwar zur Kontrolle beim Eintritt in Sicherheitsbereiche, nicht jedoch im Rahmen der Arbeitszeiterfassung verarbeitet werden können (siehe auch die Entscheidung des Arbeitsgerichts Berlin vom 19.10.2019, AZ 29 Ca 5451/19 mit Verweis auf Gola / Heckmann, 13. Auflage 2019, Rn. Nr. 157 zu § 26 BDSG, abrufbar unter https://www.iww.de/quellenmaterial/id/213545).

17.
Darf eine Arbeitgeberin auf ihrer Unternehmenswebseite die Kontaktdaten (Name, dienstliche Telefonnummer, dienstliche E-Mail-Adresse, Funktion) ihrer Beschäftigten veröffentlichen?

Diese Veröffentlichung muss für die Zwecke der Durchführung des Arbeitsverhältnisses erforderlich sein. Hierzu wird die Ansicht vertreten, dass die Kontaktdaten von Arbeitnehmern und Arbeitnehmerinnen, zu deren Aufgaben es gehört als Ansprechpartner bzw. Ansprechpartnerinnen zu fungieren, veröffentlicht werden dürfen. Dementsprechend können Name, dienstliche Telefon- und Faxnummer, E-Mail-Adresse auch ohne Einwilligung veröffentlicht werden, sofern die entsprechenden Beschäftigten für den Außenkontakt verantwortlich sind und die Daten daher dritten Personen bekannt sein müssen. Die Beschäftigten müssen darüber jedoch informiert werden.

18.
Darf ein Arbeitgeber auf seiner Unternehmenswebseite Fotografien veröffentlichen, die seine Arbeitnehmer und Arbeitnehmerinnen abbilden?

Bildnisse dürfen nur mit Einwilligung des Betroffenen veröffentlicht werden. Möchte ein Arbeitgeber daher Fotos seiner Beschäftigten auf der Webseite veröffentlichen, muss er zuvor die freiwillige informierte Einwilligung einholen. Die Freiwilligkeit der Einwilligung ist im Rahmen eines Arbeitsverhältnisses allerdings stets mit Schwierigkeiten behaftet. Seitens der Aufsichtsbehörden wird Freiwilligkeit bei einem wirtschaftlichen Vorteil und Zusatzleistungen des Arbeitgebers (beispielsweise die private Nutzung dienstlicher Fahrzeuge) unterstellt. Der Arbeitgeber muss ansonsten die Freiwilligkeit nachweisen können. Dies bedeutet, dass er den Nachweis führen muss, dass sich kein Mitarbeiter bzw. keine Mitarbeiterin „gezwungen" sieht, in die jeweilige Veröffentlichung der Fotografien einzuwilligen.

….. und zum Schluss ein kurzes Fazit: Ein Gesetz zum Beschäftigtendatenschutz ist wünschenswert.