Inhaltsübersicht

Information

1. Allgemeines

Der **Datenschutz im Beschäftigungsverhältnis** ist für viele Arbeitgeber und Personaler ein Buch mit mehr als sieben Siegeln. Die maßgeblichen Bestimmungen von Datenschutz-Grundverordnung (EU-DSGVO) und Bundesdatenschutzgesetzes (BDSG) sind oft **kaum verständlich**. Das Echo dazu in der Öffentlichkeit ist vielschichtig. Trotzdem: Bange machen gilt nicht. Selbstverständlich müssen EU-DSGVO- und BDSG und der Datenschutz im Beschäftigungsverhältnis sehr **ernst genommen** werden. Manchmal sieht es allerdings so aus, dass mit der Begründung "Datenschutz" viele vernünftige Entwicklungen verhindert oder zumindest hinausgezögert werden. Das will weder der EU- noch der nationale Gesetzgeber.

Praxistipp:

"Es wird nichts so heiß gegessen, wie es gekocht wird", sagt der Volksmund. Da hat er nicht ganz Unrecht. Gerade beim Thema Datenschutz und EU-DSGVO werden in den Medien wahre Horrorszenarien aufgerufen: das anonyme Zeugnis ohne Angabe von Alter und Geschlecht, der Hochhauseingang ohne Namensschilder, die fehlende Teilnehmerliste einer Fortbildungsveranstaltung oder die schriftliche Einwilligung aller Konzertbesucher für die Aufnahmen des Pressefotografen. Und das alles unter Berufung auf den Datenschutz? Das können weder EU- noch nationaler Gesetzgeber gewollt haben. Man sollte es nicht übertreiben und das Arbeitsleben mit einem falsch verstandenen Datenschutz noch schwerer machen.

Die EU-DSGVO gilt nach Art. 288 Abs. 2 AEUV unmittelbar und verdrängt insoweit das BDSG (s. dazu Gliederungspunkt 2.) Bei Anwendung der zu beachtenden Datenschutzbestimmungen sollte man ohnehin immer in **beide Regelwerke** gucken. Sie ergänzen sich und im nationalen BDSG nicht angesprochene Fragen lassen sich mit einem Blick in die EU-DSGVO beantworten. Für Arbeitgeber und Personaler steht besonders der **Datenschutz im Beschäftigungsverhältnis** im Fokus (s. dazu Gliederungspunkt 3.). Die Verarbeitung personenbezogener Beschäftigtendaten ist nach Maßgabe des § 26 Abs. 1 BDSG u.a. zulässig, wenn sie für Zwecke des Beschäftigungsverhältnisses - oder nach § 26 Abs. 2 BDSG - mit **Einwilligung des Arbeitnehmers** erfolgt. EU-DSGVO und BDSG sehen eine Menge von **Arbeitgeberpflichten** und **Arbeitnehmerrechten** vor (s. dazu die Stichwörter Datenschutz - Arbeitgeberpflichten und Datenschutz - Arbeitnehmerrechte). Zudem ist auf die Rechtsprechung des BAG und der Instanzgerichte zu achten (s. dazu Gliederungspunkt 4.)

2. Die EU-DSGVO und BDSG-Vorgaben

Die wesentlichen **Grundlagen des Datenschutzes** sind

- die EU-DSGVO (= 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**) und
- das BDSG (= **Bundesdatenschutzgesetz**).

Die EU-DSGVO will den **Schutz natürlicher Personen** bei der **Verarbeitung ihrer personenbezogenen Daten** sicherstellen (Art. 1 Abs. 1 EU-DSGVO). Sie "schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten" (Art. 1 Abs. 2 EU-DSGVO). Das BDSG ist das in nationales Recht gegossene EU-Datenschutzrecht mit eigenen Regelungen. Bei Anwendung der nationalen Bestimmungen ist immer § 1 Abs. 5 BDSG zu beachten:

> "Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweils geltenden Fassung, unmittelbar gilt."

§ 1 Abs. 6 BDSG stellt für den **Anwendungsbereich** der EU-DSGVO klar, dass ihr **unmittelbare Geltung** i. S. des Art. 288 Abs. 2 AEUV zukommt.

Praxistipp:

> Bei Anwendung der BDSG-Bestimmungen empfiehlt es sich, die EU-DSGVO immer mitzulesen. Zum Teil wiederholt das BDSG deren Text nur, zum Teil hat das BDSG aber auch Lücken, die durch die EU-DSGVO zu schließen sind. Manchmal ist sogar direkt auf die EU-DSGVO zuzugreifen, weil das nationale Datenschutzrecht keine Regelung enthält.

Das BDSG zielt in erster Linie auf die Datenverarbeitung (Definition in § 46 Nr. 2 BDSG und Art. 4 Nr. 2 EU-DSGVO) durch **öffentliche Stellen**. Für **nichtöffentliche Stellen** wie den Arbeitgeber gilt das Bundesdatenschutzgesetz gemäß § 1 Abs. 1 Satz 2 BDSG

> "für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten."

§ 2 BDSG enthält einen umfangreichen **Katalog von Begriffsbestimmungen** zum **Adressatenkreis**, der durch § 46 BDSG mit seinen Begriffsbestimmungen zur praktischen **Durchführung des Datenschutzes** umfangreich ergänzt wird (s. dazu auch Art. 4 EU-DSGVO). Zentrale Begriffe sind **"personenbezogen Daten"** - das sind

> "alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann" -

und **"Verarbeitung"** - das ist jeder

> "mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung".

Die BDSG-Begriffsbestimmungen werden im Stichwort Datenschutz - Begriffsbestimmungen erläutert. Das Stichwort Datenschutz - Datenverarbeitung stellt eine breite Palette - vom **Erfassen** über das **Speichern** bis hin zum **Vernichten** - von **Verarbeitungsmöglichkeiten** vor. Öffentliche wie nichtöffentliche Stellen sind bei Vorliegen der gesetzlichen Voraussetzungen verpflichtet, einen **Datenschutzbeauftragten** zu benennen. Dazu mehr im Stichwort Datenschutz - Datenschutzbeauftragter .

Zentrale Bedeutung für das **Arbeitsrecht** haben § 26 BDSG - "Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses " - und Art. 88 EU-DSGV - "Datenverarbeitung im Beschäftigungskontext". Darauf wird im nachfolgenden Gliederungspunkt 3. noch näher eingegangen. Auf eine weitere Vorstellung der EU-DSGVO- und BDSG-Bestimmungen außerhalb des Arbeitsrechts wird an dieser Stelle verzichtet und ein aufmerksames Lesen beider Regelwerke empfohlen.

3. Der Datenschutz im Arbeitsverhältnis

Die EU-DSGVO erlaubt den Mitgliedsstaaten in Art 88 Abs. 1,

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

vorzusehen. Das hat der nationale Gesetzgeber der Republik z.B. mit § 26 BDSG getan (s. dazu das Stichwort Datenschutz - Beschäftigungsverhältnis). Hier hat er die **Grundlinien** für die Verarbeitung personenbezogener Beschäftigtendaten für **Zwecke des Beschäftigungsverhältnisses** gezogen. § 26

Abs. 1 Satz 1 BDSG erlaubt die Datenverarbeitung, wenn sie

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

erforderlich ist. Zur **Aufdeckung einer Straftat** dürfen personenbezogene Beschäftigtendaten nur dann verarbeitet werden, wenn

- zu dokumentierende tatsächliche Anhaltspunkte
- den Verdacht begründen,
- dass die betroffene Person
- im Beschäftigungsverhältnis eine Straftat begangen hat,
- die Verarbeitung zur Aufdeckung erforderlich ist und
- das **schutzwürdige Interesse des Beschäftigten** an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind (so: § 26 Abs. 1 Satz 2 BDSG).

Neben der oder über die nach § 26 Abs. 1 BDSG erlaubte Datenverarbeitung dürfen personenbezogene Beschäftigtendaten auch verarbeitet werden, wenn eine **Einwilligung des Beschäftigten** vorliegt (§ 26 Abs. 2 BDSG) - an die jedoch strenge Anforderungen gestellt werden (s. dazu das Stichwort Datenschutz - Einwilligung).

Beschäftigte i.S.d. BDSG sind nach dessen § 26 Abs. 8 Satz 1 u.a.

- **Arbeitnehmer** (einschließlich Leiharbeitnehmer im Verhältnis zum Entleiher),
- zur ihrer Berufsbildung Beschäftigte,
- arbeitnehmerähnliche Personen und
- Beamte (§ 26 Abs. 8 Satz 1 Nr. 8 BDSG).

Und wichtig: "**Bewerberinnen und Bewerber** für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte" (§ 26 Abs. 8 Satz 2 BDSG).

Eine wichtige Rolle beim Beschäftigtendatenschutz nehmen nach der EU-DSGVO und dem BDSG die **Tarifvertragsparteien, Betriebs- und Personalräte** ein:

> "Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten" - so: § 26 Abs. 4 BDSG .

Und der von § 26 Abs. 4 BDSG angesprochene Art. 88 Abs. 2 EU-DSGVO sieht vor:

> "Diese Vorschriften umfassen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz."

Mehr dazu im Stichwort Datenschutz - Mitbestimmung .

Die gesetzlichen Datenschutzbestimmungen geben **Arbeitgebern** eine Menge **Pflichten** auf. Unter anderem müssen sie

- für eine rechtmäßige und transparente Datenverarbeitung sorgen (Art. 5 Abs. 1 lit. a) EU-DSGVO , § 47 Nr. 1 BDSG),
- die **Zweckbindung** der Datenverarbeitung beachten (Art. 5 Abs. 1 lit. b) EU-DSGVO , § 47 Nr. 2 BDSG),
- die Datenverarbeitung via Datenvermeidung und -sparsamkeit auf ein Minimum beschränken (Art. 5 Abs. 1 lit. c) EU-DSGVO , § 47 Nr. 3 BDSG)
- für die **Richtigkeit** der verarbeiteten Daten sorgen (Art. 5 Abs. 1 lit. d) EU-DSGVO , § 47 Nr. 4 BDSG),
- die Speicherung auf das Notwendigste begrenzen (Art. 5 Abs. 1 lit. e) EU-DSGVO , § 47 Nr. 5 BDSG) und
- für die **Sicherheit** der Datenverarbeitung sorgen (Art. 5 Abs. 1 lit. f) EU-DSGVO , § 47 Nr. 6 BDSG).

Die einzelnen Arbeitgeberpflichten werden ausführlich im Stichwort Datenschutz - Arbeitgeberpflichten vorgestellt. Teils spiegelbildlich zu den Pflichten des Arbeitgebers ist in der EU-DSGVO und im BDSG eine Vielzahl von **Arbeitnehmerrechten** verankert. Dazu gehören u. a. Ansprüche auf

- **Aufklärung**
- Auskunft

- Benachrichtigung (Art. 34 EU-DSGVO , § 56 BDSG)
- Berichtigung (Art. 16 Abs. 1 EU-DSGVO , § 58 BDSG)
- Einschränkung (Art. 18 EU-DSGVO , § 58 BDSG)
- **Information** (Art. 13 u. Art. 14 EU-DSGVO , § 33 BDSG)
- **Löschung** (§§ 35 Abs. 1 , 58 Abs. 2 BDSG)
- Schadensersatz (§ 83 Abs. 1 Satz 1 BDSG)
- Unterlassung (aus §§ 823 Abs. 1 , 1004 BGB) und
- Widerruf (Art. 7 Abs. 3 EU-DSGVO , § 51 Abs. 3 BDSG).

Ab dem 01.12.2021 werden Datenschutz und Fernmeldegeheimnis im Bereich der Telekommunikation durch das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien - **Telekommunikation-Telemedien-Datenschutz-Gesetz** (TTDSG) - v. 23.06.2021 geregelt (s. dazu BGBL. I 2021, 1982 ff.).

Weitere Informationen zu den Arbeitnehmerrechten sind im Stichwort Datenschutz - Arbeitnehmerrechte hinterlegt.

4. Rechtsprechungs-ABC

An dieser Stelle werden einige der interessantesten **Entscheidungen** zu allgemeinen Fragen des Datenschutzes **in alphabetischer Reihenfolge** nach Stichwörtern geordnet vorgestellt.

4.1 Akteneinsicht

Das Hessische Datenschutzgesetz - HDSG - sieht in § 34 Abs. 1 vor: "Der Dienstherr oder Arbeitgeber darf Daten seiner Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsieht. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts anderes geregelt ist, auf Angestellte und Arbeiter im öffentlichen Dienst entsprechend anzuwenden." Nutzt der Arbeitgeber **Daten aus einer staatsanwaltschaftlichen Ermittlungsakte**, ist das nach § 34 Abs. 1 HDSG nicht verboten. Es ist aus datenschutzrechtlichen Gründen auch nicht verboten, dass sich der Arbeitgeber von den maßgeblichen Vorgängen **Kopien** macht, um die Durchführung **arbeitsrechtlicher Maßnahmen** zu prüfen (LAG Hessen, 10.07.2015 - 14 Sa 1119/14) .

4.2 Auskunftsklage

Wer eine Klage erhebt, muss nach § 253 Abs. 2 Nr. 2 ZPO einen "bestimmten" Antrag stellen. Das Gesetz sagt nicht, was ein **bestimmter Antrag** ist. Die EU-DSGVO gibt betroffenen Personen in Art. 15 Abs. 1 Satz 1 Halbs. 1 das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, "ob sie betreffende personenbezogene Daten verarbeitet werden". Ist das der Fall, hat die betroffene Person darüber hinaus "ein **Recht auf Auskunft** über diese personenbezogenen Daten und" auf die in lit. a) bis lit. h) vorgegebenen Informationen. Das bedeutet für § 253 Abs. 2 Nr. 2 ZPO : "Ein Klageantrag, der ergänzend zum Wortlaut von Art. 15 Abs. 1 Halbs. 2 DSGVO **auslegungsbedürftige Begriffe** enthält, über deren Inhalt nicht behebbare Zweifel bestehen, ist nicht hinreichend bestimmt" (BAG, 16.12.2021 - 2 AZR 235/21 - Leitsatz).

4.3 Auskunftsrecht

Das Betriebsverfassungsrecht gibt Arbeitnehmern in § 83 Abs. 1 Satz 1 BetrVG das Recht, Einsicht in seine **Personalakte** zu nehmen - und das gesetzlich uneingeschränkt. Trotzdem kann es Fälle geben, in denen das **Einsichtsrecht eingeschränkt** werden muss. "Der Anspruch eines Arbeitnehmers gegenüber seinem Arbeitgeber auf Auskunftserteilung gem. Art. 15 Abs. 1 DSGVO auf personenbezogene Leistungs- und Verhaltensdaten kann im Einzelfall durch überwiegende **berechtigte Interessen Dritter** an einer Geheimhaltung beschränkt sein. Ob diese Interessen einer Auskunftserteilung entgegenstehen, ist durch eine Interessenabwägung im konkreten Einzelfall zu klären" (LAG Baden-Württemberg, 20.12.2018 - 17 Sa 11/18 - Leitsatz - mit dem Ergebnis, dass der Arbeitgeber hier keine Interessen Dritter - z.B. anderer Mitarbeiter oder interne Ermittlungen - entgegenhalten konnte).

4.4 Betriebsrats-PC

"1. Die **Konfiguration** des Betriebsrats-PC einschließlich der Anmeldeprozedur bestimmt der Betriebsrat grundsätzlich allein. 2. Aufgrund des Strukturprinzips der Betriebsverfassung, das jede Betriebspartei ihre Sachen selbst regelt, gelten die datenschutzrechtlichen Bestimmungen des Betriebes für die Arbeit am Betriebsrats-PC nur, soweit der Betriebsrat diese für **sachgerecht** erachtet. 3. Der Betriebsrat kann bei der Verarbeitung personenbezogener Daten unter Beachtung des Persönlichkeitsrechts der betroffenen Beschäftigten **selbst** die datenschutzrechtlichen Details bestimmen. 4. Das Bundesdatenschutzgesetz ist subsidiär zum Betriebsverfassungsgesetz (§ 1 Abs. 3 BDSG a.F.)" - (LAG Berlin-Brandenburg, 04.03.2011 - 10 TaBV 1984/10 - Leitsätze).

4.5 Datenschutz als Verfolgungshindernis

Der vereinfachte Fall: Arbeitgeber A betrieb einen **Tabak- und Zeitschriftenhandel** mit Lottoannahmestelle. In seiner Verkaufsstelle war eine **offene Video-Überwachung** installiert. A bezweckte damit den Schutz seines Eigentums vor Straftaten Dritter und seiner Arbeitnehmer. Im dritten Quartal 2016 stellte A einen **Warenschwund** fest und werte deswegen seine Videoaufzeichnungen aus - auch welche aus Februar 2016. Verkäuferin V geriet danach in Verdacht und bekam die außerordentliche Kündigung "wegen der begangenen Straftaten ". V meinte u.a., A hätte die Aufzeichnungen aus Februar nicht verwerten dürfen, weil sie nach datenschutzrechtlichen Bestimmungen längst hätten gelöscht sein müssen.

Das BAG sah sich nicht veranlasst, ein **Verwertungsverbot** anzunehmen. "Der rechtmäßig gefilmte Vorsatztäter ist in Bezug auf die Aufdeckung und Verfolgung seiner materiell-rechtlich noch verfolgbaren Tat **nicht schutzwürdig**. Er wird dies auch nicht durch bloßen Zeitablauf. Das allgemeine Persönlichkeitsrecht kann nicht zu dem alleinigen Zweck in Anspruch genommen werden, sich vor dem Eintritt von Verfall, Verjährung oder Verwirkung der Verantwortung für vorsätzlich rechtswidriges Handeln zu entziehen" (s. dazu BGH, 24.11.1981 - VI ZR 164/79). Solange die Rechtsverfolgung materiell-rechtlich noch möglich ist, wird das erhebliche - durch Art. 12 und Art. 14 GG geschützte - auf eine vorsätzliche Schädigungshandlung zielende **Verarbeitungs- und Nutzungsinteresse** des Arbeitgebers nicht geschmälert. Der Arbeitgeber ist nicht verpflichtet, Aufzeichnungen aus einer offenen Video-Überwachung "laufend vollumfänglich" zu prüfen, um relevante Szenen weiterzuverarbeiten (BAG, 23.08.2018 - 2 AZR 133/18) .

4.6 Datenschutzrechtliche "Bedenken"

Das Betriebsverfassungsgesetz verpflichtet **Mitglieder und Ersatzmitglieder des Betriebsrats** in § 79 Abs. 1 Satz 1 BetrVG , "**Betriebs- oder Geschäftsgeheimnisse**, die ihnen wegen ihrer Zugehörigkeit zum Betriebsrat bekannt geworden sind und vom Arbeitgeber ausdrücklich als geheimhaltungsbedürftig

bezeichnet worden sind, nicht zu offenbaren und nicht zu verwerten" - auch nicht nach ihrem Ausscheiden (§ 79 Abs. 1 Satz 2 BetrVG). Daneben besteht eine arbeitsvertragliche **Pflicht zu Verschwiegenheit** und sich aus den §§ 16 ff. UWG ergebende Verschwiegenheitspflichten. "Selbst wenn im Falle der Weitergabe von Geschäftsgeheimnissen des Trägerunternehmens etwa an den Vertragsarbeitgeber des Gesamtbetriebsratsmitglieds diesem keine arbeitsvertraglichen Sanktionen drohen, ist das Interesse des Trägerunternehmens an der Geheimhaltung ihrer Geschäftsgeheimnisse ausreichend durch §§ 79 , 120 BetrVG sowie §§ 16 ff. UWG geschützt" (LAG Hessen, 11.12.2017 - 16 TaBV 95/17) .

4.7 Einsicht in Arbeitnehmerdateien

"1. Der dringende Verdacht einer Pflichtverletzung kann eine ordentliche Kündigung **aus Gründen in der Person** des Arbeitnehmers iSv. § 1 Abs. 2 KSchG sozial rechtfertigen. 2. Die Einsichtnahme in auf einem Dienstrechner des Arbeitnehmers gespeicherte und **nicht als "privat" gekennzeichnete** Dateien setzt **nicht zwingend** einen durch Tatsachen begründeten Verdacht einer Pflichtverletzung voraus" (BAG, 31.01.2019 - 2 AZR 426/18 - Leitsätze).

4.8 Erforderlichkeit

Eine Datenverarbeitung ist nach § 32 Abs. 1 Satz 1 BDSG (a.. = § 26 Abs. 1 Satz 1 BDSG n.F.) nur "erforderlich", wenn der Arbeitgeber an der Erhebung, Verarbeitung oder Nutzung ein **berechtigtes Interesse** hat, das aus dem bestehenden Arbeitsverhältnis abzuleiten ist. Es muss ein **Zusammenhang** mit der Erfüllung von aus dem Beschäftigungsverhältnis folgenden Arbeitgeber- und Arbeitnehmerpflichten erkennbar sein (s. dazu BAG, 07.09.1995 - 8 AZR 828/93). Dabei darf die Verarbeitung der Beschäftigtendaten für den betroffenen Mitarbeiter nicht zu einer übermäßigen Belastung führen und muss dem **Informationsinteresse des Arbeitgebers** entsprechen. In das allgemeine Persönlichkeitsrecht des Arbeitnehmers eingreifende Maßnahmen müssen "einer Abwägung der beiderseitigen Interessen nach dem Grundsatz der Verhältnismäßigkeit standhalten" (s. dazu BAG, 07.09.1995 - 8 AZR 828/93 - und BAG, 22.10.1986 - 5 AZR 660/85). Danach muss der Arbeitgebereingriff erforderlich, geeignet und "unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen" sein, "den erstrebten Zweck zu erreichen" (BAG, 17.11.2016 - 2 AZR 730/15 - mit Hinweis auf BAG, 15.04.2014 - 1 ABR 2/13 (B) - und BAG, 29.06.2004 - 1 ABR 21/03).

4.9 Erhebungszweck

Erhebt der Arbeitgeber Daten, um den konkreten **Verdacht einer schweren Pflichtverletzung** aufzuklären, erfolgt diese Datenerhebung "für Zwecke des Beschäftigungsverhältnisses" i.S.d. § 32 Abs. 1 Satz 1 BDSG (a.F. = § 26 Abs. 1 Satz BDSG n.F.). § 32 Abs. 1 Satz 1 BDSG a.F. kodifiziert wie § 32 Abs. 1 Satz 2 BDSG (a.F. = § 26 Abs. 1 Satz 2 BDSG n.F.) die bis dahin von der Rechtsprechung entwickelten Grundsätze zum **Schutz des allgemeinen Persönlichkeitsrechts** im Arbeitsverhältnis (s. dazu BAG, 17.11.2016 - 2 AZR 730/15 - und BT-Drs. 16/13657 S. 21). Die Begründung des Gesetzes nimmt zur Ausgestaltung des Erforderlichkeitsmaßstabs für die "Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zur Durchführung oder Beendigung eines Beschäftigungsverhältnisses auf die Entscheidungen des Bundesarbeitsgerichts vom 22. Oktober 1986 (- 5 AZR 660/85 - BAGE 53, 226) und 7. September 1995 (- 8 AZR 828/93 - BAGE 81, 15) Bezug." Danach darf "sich der Arbeitgeber bei seinen Beschäftigten nicht nur über Umstände informieren oder Daten verwenden, um seine vertraglichen Pflichten ihnen gegenüber erfüllen zu können, wie z.B. Pflichten im Zusammenhang mit der Personalverwaltung, Lohn- und Gehaltsabrechnung, sondern auch, um seine im Zusammenhang mit der Durchführung des Beschäftigungsverhältnisses bestehenden Rechte wahrzunehmen, z.B. durch Ausübung des Weisungsrechts oder durch **Kontrollen der Leistung oder des Verhaltens** des Beschäftigten" (BAG, 29.06.2017 - 2 AZR 597/16 - mit Hinweis auf BT-Drs. 16/13657 S. 21).

4.10 Herausgabe personenbezogener Daten

"1. Der Informationsanspruch des Art. 15 Abs. 1 2. Halbs. DSGVO ist hinreichend bestimmt iSd. § 253 Abs. 2 Nr. 2 ZPO , wenn der Antragsteller konkret mitteilt, **welche Informationen** er im Rahmen von lit. a bis h der Norm für welche Kategorie von personenbezogenen Daten begehrt. Dasselbe gilt für den Anspruch auf **Zurverfügungstellung von Kopien** personenbezogener Daten gem. § 15 Abs. 3 Satz 1 DSGVO . 2. Eines besonderen Rechtsschutzbedürfnisses für die Geltendmachung von Ansprüchen nach Art. 15 Abs. 1 und Abs. 3 DSGVO bedarf es nicht. Es genügt grundsätzlich die Behauptung des Antragstellers, die Verantwortlichen

iSd. Art. 4 Nr. 1, 2, 7 DSGVO würden personenbezogene **Daten seiner Person** verarbeiten" (LAG Baden-Württemberg, 17.03.2021 - 21 Sa 43/20) .

4.11 Klage auf "Datenkopie" von E-Mails

Arbeitnehmer A verlangte von Arbeitgeber G Auskunft über die von G verarbeiteten personenbezogenen Daten sowie die **Überlassung** einer Kopie dieser Daten gem. Art. 15 Abs. 3 EU-DGSVO. Die Auskunft erteilte G, eine Datenkopie überließ er A nicht. Der klagte, blieb aber letztinstanzlich erfolglos. Das BAG ließ es offen, ob Art. 15 Abs. 3 EU-DGSVO tatsächlich die Überlassung von E-Mail-Kopien erfasst. Falls so ein Anspruch bestehen sollte, muss er jedenfalls mit einem hinreichend bestimmten **Klageantrag** - §§ 253 , 254 ZPO - geltend gemacht werden. "Ein Klageantrag auf Überlassung einer Kopie von E-Mails ist nicht hinreichend bestimmt iSv. § 253 Abs. 2 Nr. 2 ZPO , wenn die E-Mails, von denen eine Kopie zur Verfügung gestellt werden soll, nicht so **genau bezeichnet** sind, dass im Vollstreckungsverfahren unzweifelhaft ist, auf welche E-Mails sich die Verurteilung bezieht" (BAG, 27.04.2021 - 2 AZR 342/20 - Pressemitteilung Nr. 8/21).

4.12 Missbrauch von Kundendaten

Sensible Kundendaten müssen durch **IT-Mitarbeiter** geschützt und dürfen nicht von ihnen zu anderen Zwecken missbraucht werden. Wer als IT-Mitarbeiter gegen diese Pflicht verstößt, riskiert eine außerordentliche Kündigung. Aber auch wenn die EDV des Arbeitgebers eine Sicherheitslücke hat, darf der IT'ler nicht auf Kundendaten zugreifen und mit diesen Daten Ware für Funktionsträger dieses Kunden bestellen. Hier liegt ein eklatanter Verstoß des Arbeitnehmers gegen seine Pflicht zur Rücksichtnahme auf die Interessen des Arbeitgebers vor: ein Missbrauch des Datenzugriffs und das **Ausnutzen einer Sicherheitslücke**. Zudem liegt eine so massive **Gefährdung einer Kundenbeziehung** vor, dass insgesamt eine außerordentliche Kündigung gerechtfertigt ist (ArbG Siegburg, 15.01.2020 - 3 Ca 1793/19) .

4.13 Ohne/mit Einwilligung

Das BDSG konkretisiert und aktualisiert den Schutz des Rechts betroffener Personen auf ihre **informationelle Selbstbestimmung**. Ein Recht, das aus dem in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu verortenden **Allgemeinen Persönlichkeitsrecht** folgt. Das BDSG regelt, inwieweit in seinem Anwendungsbereich Eingriffe in die Rechte Betroffener zulässig sind (s. dazu BAG, 15.11.2012 - 6 AZR 339/11). Dies stellt § 1 Abs. 1 BDSG a.F. ausdrücklich klar. Ohne Einwilligung des Betroffenen ist die Verarbeitung seiner personenbezogenen Daten nach dem BDSG-Gesamtkonzept nur rechtmäßig, wenn eine verfassungsgemäße **Rechtsvorschrift** diese Datenverarbeitung erlaubt (§ 32 BDSG a.F. bzw. § 26 BDSG n.F. sind solche verfassungsgemäße Vorschriften, Anm. d. Verf.). Ohne einschlägige Ermächtigungs- bzw. Rechtsgrundlage ist die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten unzulässig (BAG, 12.02.2015 - 6 AZR 845/13 - mit Hinweis auf BAG, 20.06.2013 - 2 AZR 546/12 und § 4 Abs. 1 BDSG a.F.).

4.14 Polizeiliche Videoaufnahmen

"1. Art. 3 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum **Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Aufzeichnung von Polizeibeamten in einer Polizeidienststelle auf Video während der **Aufnahme einer Aussage** und die **Veröffentlichung** des so aufgezeichneten Videos auf einer Video-Website, auf der die Nutzer Videos versenden, anschauen und teilen können, in den Anwendungsbereich dieser Richtlinie fällt."

"2. Art. 9 der Richtlinie 95/46 ist dahin auszulegen, dass ein Sachverhalt wie der des Ausgangsverfahrens, d.h. die Aufzeichnung von Polizeibeamten **in einer Polizeidienststelle** auf Video während der Aufnahme einer Aussage und die Veröffentlichung des so aufgezeichneten Videos auf einer **Video-Website**, auf der die Nutzer Videos versenden, anschauen und teilen können, eine Verarbeitung personenbezogener Daten allein **zu journalistischen Zwecken** im Sinne dieser Bestimmung darstellen kann, sofern aus diesem Video hervorgeht, dass diese Aufzeichnung und diese Veröffentlichung ausschließlich zum Ziel hatten, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten, was zu prüfen Sache des vorlegenden Gerichts ist" (EuGH, 14.02.2019 - C-345/17 - Leitsätze - Lettland).

4.15 Private Telefonnummer

"1. Die **Erhebung**/**Erfassung** der privaten Mobiltelefonnummer eines/*einer Arbeitnehmers/*in gegen seinen*ihren Willen ist wegen des darin liegenden äußerst schwerwiegenden Eingriffs in das allgemeine Persönlichkeitsrecht des/*der Arbeitnehmers/*in nur dann **ausnahmsweise zulässig**, wenn der*die Arbeitgeber*in ohne Kenntnis der Mobiltelefonnummer im Einzelfall eine legitime Aufgabe, für die der*die Arbeitnehmer*in eingestellt ist, nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und ihm eine andere Organisation der **Aufgabenerfüllung** nicht möglich oder nicht zumutbar ist. (...) . Verweigert ein*e Arbeitnehmer*in die datenschutzrechtlich unzulässige Erfassung der Mobiltelefonnummer hat er*sie einen Anspruch auf Rücknahme und Entfernung einer deshalb erteilten Abmahnung aus der Personalakte" (LAG Thüringen, 16.05.2018 - 6 Sa 442/17 - 1. und 3. Leitsatz).

4.16 Recht auf informationelle Selbstbestimmung

Arbeitnehmer haben auch (und gerade) **im Arbeitsverhältnis** ein Recht auf informationelle Selbstbestimmung. Dieses Recht wird aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet. Es garantiert dem **Grundrechtsträger**, dass er selbst darüber entscheiden darf, welche persönlichen Daten er preisgibt und wie und wofür diese Daten verwendet werden (s. dazu BVerfG, 11.03.2008 - 1 BvR 2074/05 - und BAG, 17.11.2016 - 2 AZR 730/15). Das BDSG und die Datenschutzgesetze der Bundesländer regeln die Zulässigkeit der Datenverarbeitung in der Republik und den einzelnen Ländern. Sie konkretisieren und aktualisieren den Schutz des Rechts auf informationelle Selbstbestimmung. Sie regeln, in welchem Umfang im Anwendungsbereich des jeweiligen Gesetzes **Eingriffe** durch öffentliche und nichtöffentliche Stellen i.S.d. § 1 Abs. 2 BDSG (a.F.) bzw. nach Landesrecht zulässig sind. Für die Verwendung von Gesundheitsdaten personenbezogener Art - sensitive Daten i.S.v. § 3 Abs. 9 BDSG a.F. - gibt es spezielle Regelungen in § 28 VI ff. BDSG (a.F. = § 22 BDSG n.F.). Eine "Datenerhebung" i. S. des Datenschutzrechts liegt nicht vor, wenn der Arbeitnehmer eine "vermeintliche Drohung [hier mit einer Selbsttötung] von sich aus erklärt (BAG, 29.06.2017 - 2 AZR 47/16) .

4.17 Schadensersatz

"Jede Person", sagt Art. 82 Abs. 1 EU-DGSVO, "der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat **Anspruch** auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter ." Und Art. 82 Abs. 2 Satz 1 EU-DSGVO ergänzt: "Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde," Aber: "Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Art. 82 Abs. 3 EU-DSGVO). Trotzdem bedeutet das für den Geschädigten: "**Voraussetzung** für einen Schadensersatzanspruch gemäß Art. 82 Abs. 1 DSGVO ist der **Nachweis eines konkreten (auch immateriellen) Schadens**" (OLG Frankfurt, 02.03.2022 - 13 U 206/20 - Leitsatz).

4.18 Schadensersatz/Schmerzensgeld - 1

Jede Person, der **wegen eines Verstoßes** gegen die EU-DSGVO ein materieller oder immaterieller Schaden entstanden ist, hat nach Art. 82 Abs. 1 EU-DSGVO Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter . Z.B. dann, wenn der Arbeitgeber das **Foto eines Mitarbeiters** nach dessen Ausscheiden noch als PDF zugänglich macht. Gehört zum Schaden auch die Erstattung der Kosten, die dem Arbeitnehmer durch Beauftragung des Anwalts entstanden sind, der seinen Schadensersatzanspruch geltend machen soll? Eher nicht. Wozu gibt es im erstinstanzlichen Urteilsverfahren vor den Arbeitsgerichten das so genannte **Kostenprivileg**. Daher: "Schadensersatz nach Art. 82 DSGVO hindert die Kostenregelung aus § 12a ArbGG nicht" (LAG Köln, 14.09.2020 – 2 Sa 358/20 – Leitsatz – mit dem Ergebnis, dass der Arbeitnehmer hier nur 300,00 EUR Schmerzensgeld zugesprochen bekam).

4.19 Schadensersatz/Schmerzensgeld - 2

Art. 82 Abs. 1 EU-DSGVO gibt jeder Person, der wegen eines EU-DSGVO-Verstoßes ein **materieller oder immaterieller Schaden** entstanden ist, einen Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Beide Schäden – sowohl der materielle als auch der immaterielle – sind

ersatzfähig. Der EuGH-Rechtsprechung zufolge muss der geschuldete Schadensersatz gerade bei immateriellen Schäden eine **abschreckende Wirkung** haben (s. dazu EuGH, 17.12.2015 – C-407/14). Dabei ist die bisherige deutsche Rechtsprechung, die einen immateriellen Schadensersatzanspruch erst dann bejahte, wenn eine schwerwiegenden Persönlichkeitsrechtsverletzung vorlag, nicht mehr maßgeblich. So setzt ein immaterieller Schadensersatz nach Art. 82 Abs. 1 EU-DSGVO wegen rechtswidriger Detektivüberwachung aktuell **keine schwerwiegende Persönlichkeitsrechtsverletzung** mehr voraus (LAG Hessen, 18.10.2021 – 16 Sa 380/20).

4.20 Sensitive Daten

Das bis einschließlich 24.05.2018 geltende Bundesdatenschutzgesetz ließ in § 28 Abs. 6 Nr. 3 BDSG (a.F. = § 22 BDSG n.F.) das **Erheben, Verarbeiten und Nutzen** besonderer Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG für eigene Geschäftszwecke auch **ohne Einwilligung** des Betroffenen zu, "wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt." Da es sich hier um **besondere Kategorien** personenbezogener Daten handelt, ist § 32 BDSG (a.F. = § 26 BDSG n.F. "Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses ") nicht einschlägig. Er sieht zwar eine Regelung über den Schutz personenbezogener Daten im Beschäftigungsverhältnis vor, sein Regelungsgegenstand erfasst aber nur personenbezogene Daten , keine sensitiven i.S.d. § 3 Abs. 9 BDSG (BAG, 07.02.2012 - 1 ABR 46/10) .

4.21 Suchmaschine

"Die Bestimmungen von Art. 8 Abs. 1 und 5 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum **Schutz natürlicher Personen** bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sind dahin auszulegen, dass das darin enthaltene Verbot oder die darin enthaltenen Beschränkungen der **Verarbeitung besonderer Kategorien** personenbezogener Daten - vorbehaltlich der in dieser Richtlinie vorgesehenen Ausnahmen - auch auf den Betreiber einer Suchmaschine als den für die Datenverarbeitung bei der Tätigkeit dieser Suchmaschine Verantwortlichen in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten bei Gelegenheit einer **Prüfung** anwendbar sind, die der Suchmaschinenbetreiber auf Antrag der betroffenen Person unter Aufsicht der zuständigen nationalen Behörden vornimmt" (EuGH, 24.09.2019 - C-136/17 - 1. Leitsatz - Frankreich).

4.22 Verdeckte Maßnahmen

Nach dem Willen des Gesetzgebers sollte § 32 BDSG (a.F. = § 26 BDSG n.F.) die bis dahin von der Rechtsprechung für das Beschäftigungsverhältnis herausgearbeiteten Datenschutzgrundsätze nicht ändern, sondern bloß zusammenfassen (s. dazu BT-Drs. 16/13657 S. 20; BAG, 20.10.2016 - 2 AZR 395/15 - und BAG, 12.02.2015 - 6 AZR 845/13). Das - alte - BDSG ist kein 'ausgereiftes' Gesetz. Es macht einen - nachfolgenden - umfassenden **Beschäftigtendatenschutz** weder entbehrlich noch präjudiziert es ihn inhaltlich. § 32 BDSG a.F. ist nur eine **"Kodifikation der Rechtsprechungsgrundsätze"** (s. dazu BT-Drs. 16/13657 S. 20). "Nach den demgemäß in § 32 BDSG zusammengefassten Rechtsprechungsgrundsätzen sind aber - sofern weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Überwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist - **Eingriffe in das allgemeine Persönlichkeitsrecht** der Arbeitnehmer durch bspw. eine verdeckte (Video-)Überwachung nicht nur dann zulässig, wenn der konkrete Verdacht einer strafbaren Handlung besteht, sondern ebenso bei einem entsprechenden Verdacht einer anderen schweren Verfehlung zu Lasten des Arbeitgebers" (BAG, 29.06.2017 - 2 AZR 597/16 - mit Hinweis auf BAG, 27.03.2003 - 2 AZR 51/02).

4.23 Verhältnismäßigkeitsprüfung

Der frühere § 32 Abs. 1 Satz 2 BDSG a.F. (= § 26 Abs. 1 Satz 2 BDSG n.F.) hatte **keine Sperrwirkung** dahingehend, "dass eine anlassbezogene Datenerhebung durch den Arbeitgeber **ausschließlich zur Aufdeckung von Straftaten** zulässig wäre und sie nicht nach § 32 Abs. 1 Satz 1 BDSG aF zulässig sein könnte" (s. dazu BAG, 27.07.2017 - 2 AZR 681/16 ; BAG, 29.06.2017 - 2 AZR 597/16 - und § 26 Abs. 1 Satz 1 BDSG n.F.). Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten mussten allerdings nach § 32 Abs. 1 Satz 1 BDSG a.F. (= § 26 Abs. 1 Satz 1 BDSG n.F.) **"erforderlich"** sein - und

dabei hat eine volle Verhältnismäßigkeitsprüfung zu erfolgen.

"Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten müssen geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte **angemessen** sein, um den erstrebten Zweck zu erreichen." Folgerichtig dürfen **keine anderen Mittel** zur Verfügung stehen, die zur Zielerreichung gleich wirksam sind und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränken. Die Angemessenheit der Datenverarbeitung ist gewahrt, "wenn die Schwere des Eingriffs bei einer **Gesamtabwägung** nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht. Die Datenerhebung, -verarbeitung oder -nutzung darf keine übermäßige Belastung für den Arbeitnehmer darstellen und muss der Bedeutung des Informationsinteresses des Arbeitgebers entsprechen. Dies beurteilt sich ggf. für jedes personenbezogene Datum gesondert" (BAG, 31.01.2019 - 2 AZR 426/18 - mit Hinweis auf BAG, 23.08.2018 - 2 AZR 133/18).

4.24 Verwertungsverbot

In einem **Kündigungsschutzverfahren** tritt kein Verwertungsverbot zugunsten des Arbeitnehmers ein, wenn der Arbeitgeber das fragliche Beweismittel oder die maßgebliche Erkenntnis im Einklang mit den einschlägigen Datenschutzbestimmungen erlangt und weiterverwandt hat (s. dazu BAG, 23.08.2018 - 2 AZR 133/18). Bei der vorzunehmenden Interessenabwägung muss sich, wenn ein Verwertungsverbot bejaht werden soll, das Nichtverwertungsinteresse des Arbeitnehmers gegenüber dem **Verarbeitungsinteresse des Arbeitgebers** durchsetzen. Die Einsichtnahme in nicht als "privat" gekennzeichnete Dateien und nicht offenkundig als "privat" zu erkennende Dateien auf dem Dienstrechner eines Arbeitnehmers (hier: Datei Tankbelege.xls bei einem Verdacht auf Tankkartenmissbrauch) ist nicht so eingriffsintensiv, daraus ein überwiegendes **Nichtverwertungsinteresse des Mitarbeiters** zu folgern (BAG, 31.01.2019 - 2 AZR 426/18 - mit dem Ergebnis, dass hier kein Verwertungsverbot bestand).

4.25 Widerrechtliche Datenveröffentlichung

Betriebsrat B hatte **via Dropbox** Dritten Prozessakten aus einem vorherigen Kündigungsschutzverfahren zwischen ihm und Arbeitgeber A zugänglich gemacht. Die Schriftsätze enthielten u. a. personenbezogene Daten , insbesondere Gesundheitsdaten, anderer Mitarbeiter des A **unter voller Namensnennung**. Ein Grund für ihn, B's Arbeitsverhältnis nach Zustimmung des Gremiums Betriebsrat außerordentlich zu kündigen. Die Offenlegung geschützter Daten gegenüber der Betriebsöffentlichkeit durch Verwendung eines zur Verfügung gestellten Links und die damit geschaffene Möglichkeit der Verbreitung dieser Daten ohne rechtfertigenden Grund stellt eine rechtswidrige und schuldhafte **Verletzung des Persönlichkeitsrechts** der in den Schriftsätzen namentlich benannten Personen dar. B hat in diesem Fall keine berechtigten Interessen wahrgenommen – er hätte gegen die abweisende Entscheidung des Arbeitsgerichts Berufung einlegen können (LAG Baden-Württemberg, 25.03.2022 – 7 Sa 63/21) .

4.26 Zeiterfassung mit Fingerabdruck-Scanner

Der vereinfachte Fall: Arbeitgeber A führte in seiner radiologischen Praxis ein Zeiterfassungssystem ein, das mit einem Fingerabdruck-Scanner bedient wird. Mitarbeiter M, ein Medizinisch-Technischer Assistent, weigerte sich, dieses System zu nutzen. Die vereinfachte Lösung: Recht hat er. Das System erfasst **biometrische Daten**, deren Verarbeitung nach Art. 9 Abs. 2 EU-DSGVO nur ausnahmsweise erlaubt ist. Die von Art. 9 Abs. 1 EU-DSGVO verlangte **Erforderlichkeit der Verarbeitung** biometrischer Daten konnte hier nicht festgestellt werden. Ohne **Einwilligung** des Arbeitnehmers in die Datenverarbeitung ist die Zeiterfassung per Fingerabdruck - auch wenn in diesem Fall nicht der ganze Fingerabdruck, sondern lediglich Fingerlinienverzweigungen gescannt wurden - unzulässig (LAG Berlin-Brandenburg, 04.06.2020 - 10 Sa 2130/19 - mit dem weiteren Ergebnis, dass die Weigerung des Mitarbeiters keine Pflichtverletzung darstellte und die ihm vom Arbeitgeber erteilte Abmahnung aus der Personalakte zu entfernen war).