F. Beschäftigtendatenschutz und Social Media

Schrifttum: Allgemein: *Bayreuther*, Whistleblowing und das neue Hinweisgeberschutzgesetz, NZA Beilage 1/2022, 20; *Besgen*/*Prinz* (Hrsg.), Arbeiten 4.0, Datenschutz und Arbeitsrecht in der digitalisierten Arbeitswelt, 5. Aufl. 2022; *Brink*/*Joos*, Datenschutzrechtliche Folgen für den Betriebsrat nach dem Betriebsrätemodernisierungsgesetz, NZA 2021, 1440; *Byers*/*Fischer*, Rechtliche Vorgaben bei der Durchführung von sog. „Backgroundchecks“, ArbRAktuell 2022, 90; *Däubler*/*Wedde*/*Weichert*/*Sommer*, EU-DSGVO und BDSG, 3. Aufl. 2024 (zit.: DWWS/*Bearbeiter*); *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Der Ratgeber – Beschäftigtendatenschutz, 4. Aufl. 2020; *Dzida*, Einblicksrecht des Betriebsrats in Bruttoentgeltlisten im Spannungsverhältnis zum Beschäftigtendatenschutz, RdA 2020, 295; *Dzida*/*Storms*, „Richter in eigener Sache“ – der Betriebsratsvorsitzende darf nicht zugleich Datenschutzbeauftragter sein, BB 2023, 2548; *Gola*, Handbuch Beschäftigtendatenschutz, 9. Aufl. 2022; *Grau*, Der Umgang mit Beschäftigtendaten bei Betriebsübernahmen und Unternehmenskäufen nach der Datenschutz-Grundverordnung, in Festschrift Willemsen, 2018, S. 147; *Grimm*/*Vitt*, Die neue datenschutzrechtliche Stellung des Betriebsrats nach Maßgabe des Betriebsrätemodernisierungsgesetzes – Über Inhalt, Reichweite und Folgen von § 79a BetrVG, ArbRB 2021, 279; *Kühling*/*Buchner*, DS-GVO BDSG 4. Aufl. 2024; *Maschmann*, Der Arbeitgeber als Verantwortlicher für den Datenschutz im Betriebsratsbüro (§ 79a BetrVG)?, NZA 2021, 834; *Malorny*, Auswahlentscheidungen durch künstlich intelligente Systeme, JuS 2022, 289; *Schmidt*/*Plote*, Die Zulässigkeit der Datenverarbeitung im betrieblichen Eingliederungsmanagement, NZA 2022, 1297; *Thüsing*, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021; *Weth*/*Herberger*/*Wächter*/*Sorge*, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 3. Aufl. 2025.

Zur EU-Datenschutzgrundverordnung: *Anton-Dyck*/*Böhm*, Aufbewahrungsfristen für BEM-Unterlagen in der Personalakte, ArbRB 2020, 280; *Brams*/*Wybitul*, Immaterieller Schadensersatz wegen Datenschutzverstößen, ArbRB 2020, 274; *Franzen*; Persönlichkeitsrecht und Datenschutz im Arbeitsverhältnis, ZfA 2019, 18; *Franzen*, Das Verhältnis des Auskunftsanspruchs nach DS-GVO zu personalaktenrechtlichen Einsichtsrechten nach dem BetrVG, NZA 2020, 1593; *Grimm*/*Kühne*, Löschkonzept nach der DSGVO, ArbRB 2018, 144; *Korinth*, Arbeitgeber zwischen Hinweisgeberschutz und datenschutzrechtlichem Auskunftsanspruch, ArbRB 2025, 22; *Leibold*, Schadensersatzansprüche sowie Inhalt und Streitwerte des Auskunftsanspruchs nach der

DSGVO, ZD 2022, 18; *Lembke/Fischels*, Datenschutzrechtlicher Auskunfts- und Kopieanspruch im Fokus von Rechtsprechung und Praxis, NZA 2022, 513; *Maschmann*, Der Anspruch auf Datenkopie: ein neues Geschäftsmodell?, NZA Beilage 1/2022, 50.

Zur Kontrolle und Überwachung von Arbeitnehmern: *Behling*, Herausforderung Datenschutz: Rechtskonforme Ausgestaltung von Terrorlisten-Screenings, NZA 2015, 1359; *Fuhlrott/Oltmanns*, Arbeitnehmerüberwachung und interne Ermittlungen im Lichte der Datenschutz-Grundverordnung, NZA 2019, 1097; *Grimm*, Überwachung im Arbeitsverhältnis: Von Befragungen bis zur GPS-Ortung – wie viel Kontrolle ist erlaubt?, jM 2016, 17; *Grimm/Schiefer*, Videoüberwachung am Arbeitsplatz, RdA 2009, 329; *Koch*, Die Rechtsprechung des Zweiten Senats des Bundesarbeitsgerichts zur prozessualen Verwertbarkeit der Ergebnisse aus verdeckten Überwachungsmaßnahmen, ZfA 2018, 109; *Vitt*, Datenschutzrechtliche Zulässigkeit von Background-Checks, BB 2024, 2868.

Zu aktuellen Entwicklungen und zu Social Media: *Aßmus/Winzer*, Mitarbeiterfotos im Intranet, auf Webseiten und in sozialen Netzwerken, ZD 2018, 508; *Fuhlrott/Oltmanns*, Social Media im Arbeitsverhältnis – Der schmale Grat zwischen Meinungsfreiheit und Pflichtverletzung, NZA 2016, 785; *Haußmann/Thieme*, Reformbedarf und Handlungsoptionen in der IT-Mitbestimmung, NZA 2019, 1612; *Herberger*, Arbeitsrechtliche Rahmenbedingungen für Corporate-Influencer, NZA 2022, 238; *Kort*, Recht des Betriebsrats auf Daten der elektronischen Personalakte, ZD 2015, 3; *Kramer*, Verwertungsverbot und sanktionsfrei Sphäre bei privaten Social-Media-Äußerungen, NZA 2024, 965; *Niklas/Köllmann*, Posten, bloggen, kommentieren – „Influencen" im Auftrag des Arbeitgebers, ArbRB 2020, 277; *Niklas/Peter*, WhatsApp & Co. – Die Messenger-Nutzung auf Diensthandys, ArbRB 2019, 50; *Reufels/Pütz*, Einsatz privater Mobilgeräte im Arbeitsverhältnis (BYOD), ArbRB 2018, 26; *Thüsing/Wurth*, Social Media im Betrieb, 2. Aufl. 2020.

Zu Big Data: *Dzida*, Big Data und Arbeitsrecht, NZA 2017, 541; *Dzida/Groh*, People Analytics im Personalbereich, ArbRB 2018, 179; *Göpfert/Brune*, Moderne Führungsinstrumente auf dem arbeitsrechtlichen Prüfstand, NZA Beilage 4/2018, 87; *Kort*, Neuer Beschäftigtendatenschutz und Industrie 4.0, RdA 2018, 24; *Malorny*, Datenschutz als Grenze KI-basierter Auswahlentscheidungen im Arbeitsrecht, RdA 2022, 170; *Rudkowski*, „Predictive policing" am Arbeitsplatz, NZA 2019, 72; *Waas*, KI und Arbeitsrecht, RdA 2022, 125.

Zu KI-Verordnung: *Frank/Heine*, Arbeitsrechtliche Dimension der KI-Verordnung, NZA 2024, 433; *Grimm/Krülls*, Die KI-Verordnung aus arbeitsrechtlicher Sicht, ArbRB 2024, 368; *Grimm/Krülls*, KI-Richtlinien im Betrieb, ArbRB 2024, 108; *Grossmann/Grunicke/Henke*, KI-Tools im Recruiting und ihre arbeitsrechtliche Implikation, BB 2024, 2229; *Günther/Gerigk/Berger*, Von Algorithmen und Arbeitnehmern: Die europarechtliche Regulierung von KI im arbeitsrechtlichen Kontext, NZA 2024, 234; *Holthausen*, Einsatz künstlicher Intelligenz im HR-Bereich und Anforderungen an die „schöne neue Arbeitswelt X.0", RdA 2023, 361; *Lang/Rheinbach*, Künstliche Intelligenz und betriebliche Mitbestimmung, BB 2024, 1396; *Martini/Wendehorst*, KI-VO – Verordnung über künstliche Intelligenz, 2024; *Müller*, Künstliche Intelligenz (KI) im Arbeitsverhältnis, öAT 2024, 26; *Reinhard*, KI in der Mitbestimmung – Wie kann das funktionieren?, ArbRB 2024, 372; *Schwartmann/Keber/Zenner*, KI-VO – Leitfaden für die Praxis, 2. Aufl. 2024; *Stramer/Thiele*, Datenschutz-Compliance beim KI-Einsatz im Unternehmen, ArbRB 2024, 375; *Witteler*, ChatGPT ein Thema für den Betriebsrat?, ZD 2023, 377; *Witteler/Moll*, Künstliche Intelligenz am Arbeitsplatz – Datenschutz und Rechte des Betriebsrats, NZA 2023, 327.

I. Normative Grundlagen und Grundbegriffe

1. Rechtsgrundlagen

1 Die **EU-Datenschutz-Grundverordnung** (DSGVO) hat zum 25.5.2018 Geltung erlangt und ist seither die wichtigste Rechtsquelle des deutschen Datenschutzrechts. Die DSGVO regelt **alle Bereich des Datenschutzrechtes** umfassend und schließt den Beschäftigungsdatenschutz im Grundsatz ein. Als **Verordnung** findet sie gegenüber Privatpersonen und Unternehmen **unmittelbare** und **zwingende** Anwendung.

2 Im Ausgangspunkt genießt die DSGVO **Anwendungsvorrang** gegenüber nationalen Gesetzen (Art. 288 AEUV). Allerdings enthält die DSGVO eine Vielzahl von **Öffnungsklauseln**, in deren Rahmen der nationale Gesetzgeber konkretisierende Regelungen erlassen darf. Das ist durch die Neufassung des **Bundesdatenschutzgesetzes** (BDSG) zum 25.5.2018 geschehen. Im Lichte der Wertungen

der DSGVO sind die Öffnungsklauseln dabei **europarechtskonform auszulegen**[1]. Die wichtigste nationale Bestimmung zum Beschäftigtendatenschutz ist **§ 26 BDSG**, welche aufgrund der Öffnungsklausel in Art. 88 DSGVO ergangen ist.

Schon lange vor Inkrafttreten der DSGVO war der **Persönlichkeitsschutz als durchdringendes Rechtsprinzip** im Arbeitsrecht anerkannt. Das allgemeine Persönlichkeitsrecht und Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG) kollidiert mit dem Grundrecht des Arbeitgebers auf wirtschaftliche Handlungs- und Betätigungsfreiheit (Art. 2 Abs. 1 GG) und auf Berufsfreiheit (Art. 12 Abs. 1 GG). Der Schutz personenbezogener Daten ist zudem nach Maßgabe von Art. 8 GrCh gewährleistet. Arbeitsvertraglich wirken die Grundrechte als Ausprägung des allgemeinen Persönlichkeitsrechts zudem über die Rücksichtnahmepflicht des § 241 Abs. 2 BGB. Daneben tritt der deliktsrechtliche Schutz als absolutes Recht nach § 823 Abs. 1 BGB[2]. 3

Andere Rechtsvorschriften des Bundes (zB das TTDSG) gehen dem BDSG vor, „soweit" sie auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Das BDSG ist also **subsidiär** anzuwenden (§ 1 Abs. 2 Satz 1 BDSG). Sie können allerdings nur dann Anwendung finden, wenn ihr Regelungsinhalt eine Öffnungsklausel der DSGVO ausfüllt. Andernfalls müssten sie selbst mit speziellerem Regelungsinhalt hinter die DSGVO zurücktreten, da die DSGVO gegenüber nationalem Recht normenhierarchisch Anwendungsvorrang genießt. Ob datenschutzrelevante Bundesgesetze nach Geltungserlangung der DSGVO weiterhin Anwendung finden – ggf. unter europarechtskonformer Auslegung – muss stets im Einzelfall geprüft werden und wird in vielen Bereichen kontrovers diskutiert. 4

Im Beschäftigungsdatenschutz können datenschutzrechtliche Ermächtigungsgrundlagen und Verarbeitungsverbote zudem durch **Kollektivvereinbarungen**, dh. durch Tarifvertrag oder durch Betriebsvereinbarung, geschaffen werden (Art. 88 DSGVO, § 26 Abs. 4 BDSG). Wegen des **Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 6 BetrVG** haben **Betriebsvereinbarungen** bei der elektronischen Verarbeitung von Beschäftigtendaten in Deutschland eine Schlüsselfunktion. 5

2. EU-Datenschutzgrundverordnung (DSGVO)

a) Anwendungsbereich

Die DSGVO gilt sachlich für die automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO) (zur Definition s. Rz. 15 f.). 6

Räumlich findet die DSGVO Anwendung, soweit die Datenverarbeitung durch ein verantwortliches Unternehmen erfolgt, das seine Niederlassung in der Europäischen Union hat (sog. „**Niederlassungsprinzip**"; Art. 3 Abs. 1 DSGVO). Dies gilt unabhängig davon, ob die Verarbeitung selbst innerhalb der EU erfolgt[3]. Ein in der EU niedergelassenes Unternehmen kann sich seinen datenschutzrechtlichen Verpflichtungen nicht dadurch entziehen, dass es Datenverarbeitungsvorgänge ins außereuropäische Ausland auslagert. Verarbeitet eine europäische Unternehmensniederlassung Beschäftigtendaten, findet die DSGVO auch dann Anwendung, wenn sich die betroffenen Beschäftigten im außereuropäischen Ausland aufhalten[4]. 7

Die DSGVO gilt zudem für Datenverarbeitungsvorgänge im außereuropäischen Ausland, die sich auf im EU-Inland befindliche Personen bezieht, sofern die Datenverarbeitung darauf zielt, diesen Personen in der EU Waren oder Dienstleistungen anzubieten oder ihr Verhalten in der EU beobachtet werden soll (sog. „**Marktortprinzip**"; Art. 3 Abs. 2 DSGVO). 8

1 HWK/*Lembke*, Art. 88 DSGVO Rz. 5.
2 MünchArbR/*Reichold*, § 94 Rz. 1, 30.
3 Paal/Pauly/*Ernst*, Art. 3 DSGVO Rz. 11; Simitis/*Hornung*, Art. 3 DSGVO Rz. 46.
4 BeckOK Datenschutzrecht/*Hanloser*, Art. 3 DSGVO Rz. 24.

b) Regelungsinhalt

9 Auf europäischer Ebene war das Datenschutzrecht in der Vergangenheit durch die EU-Datenschutzrichtlinie 95/46/EG[5] geregelt, welche durch die DSGVO umfassend abgelöst wurde (Art. 94 DSGVO). Augenscheinlichste Neuerung der DSGVO ist die massive **Verschärfung** der **Bußgeldsanktionen**: Die DSGVO erhöhte die Bußgeldrahmen gegenüber der früheren Rechtslage auf etwa das **Sechzigfache** (!). Datenschutz ist seither eine **Kernherausforderung der Unternehmens-Compliance**. Auf der Tatbestandsseite kennt die DSGVO drei Arten von bußgeldbewehrten Vorgaben:

10 Zum einen müssen Datenverarbeitungsvorgänge im Geltungsbereich der DSGVO **materiell-rechtlich** gerechtfertigt werden (Art. 6 Abs. 1 DSGVO). Ob und in welcher Form sich Datenverarbeitungen rechtfertigen lassen, hängt in den meisten Fällen von einer einzelfallbezogenen Interessenabwägung ab, bei der erhebliche Wertungsspielräume bestehen. Die meisten Fallkonstellationen sind höchstgerichtlich bislang noch nicht entschieden. Unternehmen haben gegenüber den Datenschutzbehörden derzeit große Argumentationsspielräume, sehen sich aber gleichzeitig einer ebenso großen Rechtsunsicherheit ausgesetzt.

11 Zum anderen stellt die DSGVO auch für an sich zulässige Datenverarbeitungsvorgänge eine Vielzahl **formeller Vorgaben** auf. So müssen Unternehmen ihre Datenverarbeitungsvorgänge in Verzeichnissen darstellen (Art. 30 DSGVO), gegenüber den betroffenen Personen umfangreiche Informationen erteilen (Art. 13, 14 DSGVO) und erhobene Daten nach definierten Konzepten routinemäßig löschen (Art. 17 DSGVO). Im Hinblick auf die formellen Vorgaben sind Auslegungsspielräume gering.

Schließlich räumt die DSGVO den betroffenen Personen eine Reihe von **Individualansprüchen** gegenüber den für die Datenverarbeitung Verantwortlichen ein (Art. 12 ff. DSGVO). Deren Verletzung kann zusätzlich zu **Bußgeldern** und **Schadensersatzansprüchen** (Art. 82 DSGVO) führen.

c) Öffnungsklausel nach Art. 88 DSGVO

12 Die **Öffnungsklausel** des Art. 88 Abs. 1 und Abs. 2 DSGVO gibt dem nationalen Normgeber im **Beschäftigungskontext** die Möglichkeit, **konkretisierende Sonderregelungen** zu treffen. **Zulässig** sind nationale Regelungen, die im Verhältnis zur DSGVO einen spezifischeren Regelungsinhalt aufweisen und angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Personen vorsehen[6]. Das hat zur Folge, dass das durch die DSGVO vermittelte **Schutzniveau** durch deutsche spezifische Vorschriften zum Beschäftigtendatenschutz **überschritten**[7] und (geringfügig) **unterschritten** (sehr str.)[8], aber nicht insgesamt abbedungen werden darf.

Auf Grundlage dieser Öffnungsklausel ist § 26 BDSG ergangen. Die Öffnungsklausel kann auch durch Kollektivvereinbarungen, dh. Betriebsvereinbarungen und Tarifverträge, ausgefüllt werden, sofern deren Regelungsinhalt die vorgegebenen Anforderungen erfüllt (§ 26 Abs. 4 BDSG).

Der EuGH hat 2023 entschieden, dass der zu dem § 26 Abs. 1 Satz 1 BDSG gleichlautende **hessische § 23 Abs. 1 Satz 1 HDSIG keine** spezifischere Vorschrift iSv. Art. 88 Abs. 1 DSGVO und daher nicht DSGVO-konform ist[9]. Grundsätzlich dürfen diese Bestimmungen infolge des Vorrangs des Unionsrechts nicht angewendet werden. Deshalb ist auch der zu § 23 Abs. 1 Satz 1 HDSIG wortgleiche **§ 26**

5 ABl. EU Nr. L 281/31.

6 Dazu Paal/*Pauly*, Art. 88 DSGVO Rz. 3 ff.; *Düwell*/*Brink*, NZA 2016, 655; *Tiedemann*, ArbRB 2016, 334 (336).

7 Paal/*Pauly*, Art, 88 DSGVO Rz. 4; Kühling/*Buchner*/*Maschmann*, Art. 88 DSGVO Rz. 30, 31; *Tiedemann*, ArbRB 2016, 334; *Wybitul*, NZA 2017, 413.

8 Wie hier HWK/*Lembke*, Art. 88 DSGVO Rz. 8; BeckOK Datenschutzrecht/*Riesenhuber*, Art. 88 DSGVO Rz. 67; aA Gola/Heckmann/*Pötters*, Art. 88 DSGVO Rz. 26; *Wybitul*, NZA 2017, 413.

9 EuGH v. 30.3.2023 – C-34/21, NZA 2023, 487.

Abs. 1 Satz 1 BDSG nicht mehr anzuwenden. Deutschland hat diese datenschutzrechtliche Ermächtigungsgrundlage verloren.

In der Praxis hat dies aber nur **geringe** Auswirkungen. Die Verarbeitung personenbezogener Beschäftigtendaten kann regelmäßig auf Art. 6 Abs. 1 lit. b, c und f DSGVO gestützt werden. Insbesondere die Rechtfertigung auf Rechtsgrundlage des Art. 6 Abs. 1 lit. b und f DSGVO wird übergangslos die Rechtfertigung für die Datenverarbeitung im Beschäftigungskontext darstellen können[10].

Bei § 26 Abs. 1 Satz 2 BDSG und § 26 Abs. 2 und 3 BDSG handelt es sich um spezifische Normen iSv. Art. 88 DSGVO. Diese haben also weiterhin Bestand[11].

3. Bundesdatenschutzgesetz (BDSG)

Das BDSG gilt für Datenverarbeitungsvorgänge auf dem Staatsgebiet der Bundesrepublik Deutschland (§ 1 Abs. 4 Nr. 1 BDSG) sowie für Datenverarbeitungsvorgänge durch Unternehmensniederlassungen, die auf dem Staatsgebiet der Bundesrepublik Deutschland ansässig sind („**Niederlassungsprinzip**"; § 1 Abs. 4 Nr. 2 BDSG). Nach § 1 Abs. 4 Nr. 3 BDSG soll das BDSG zudem für alle Verantwortlichen und Auftragsverarbeiter Anwendung finden, die in den Anwendungsbereich der DSGVO fallen. Allerdings ist unklar, wie diese ihrem Wortlaut nach offenkundig zu weit gefasste letztgenannte Bestimmung auszulegen ist[12]. 13

Inhaltlich bildet das BDSG kein geschlossenes Regelungssystem mehr ab, sondern enthält eine Ansammlung von Einzelregelungen, welche die DSGVO im Rahmen der Öffnungsklauseln konkretisieren oder ergänzen. Für den **Beschäftigtendatenschutz** sind – neben den Regelungen der DSGVO – die materielle Regelung des § 26 BDSG sowie die Bestimmungen zum Datenschutzbeauftragten nach §§ 38, 6 BDSG von zentraler Bedeutung. 14

4. Grundbegriffe

a) Personenbezogene Daten

„**Personenbezogene Daten**" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Diese Person wird als **„betroffene Person"** bezeichnet. Ein innerer Zusammenhang zum Arbeitsverhältnis ist nicht notwendig. 15

Sind die Daten iSd. § 3 Abs. 6 BDSG aF **„anonymisiert"**, liegen keine personenbezogenen Daten vor[13]. Anonymisiert sind Daten, wenn der Personenbezug des Datums so weit entfernt wurde, dass eine Identifizierung der betroffenen Person ausgeschlossen ist (ErwGr 26 DSGVO)[14]. An eine Anonymisierung sind unter der DSGVO hohe Anforderungen zu stellen. Ist der Personenbezug unter Hinzuziehung zusätzlicher Informationen mit einigem Aufwand noch herstellbar, liegt lediglich eine sog. **„Pseudonymisierung"** und damit weiterhin ein personenbezogenes Datum vor (Art. 4 Nr. 5 DSGVO). Pseudonymisierte personenbezogene Daten sind allerdings in aller Regel weniger schutzbedürftig, da unbefugte Verwender sie nicht zuordnen könnten. 16

b) Datenverarbeitung

Eine „**Verarbeitung**" ist jeder ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten (Art. 4 Nr. 2 DSGVO). Beispielhaft nennt die DSGVO das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Ver- 17

10 *Grimm*, ArbRB 2023, 131; *Kaufmann/Wegmann/Wieg*, NZA 2023, 740 (742).
11 *Grimm*, ArbRB 2023, 131; *Kinzinger*, DB 2024, 935.
12 Eingehend Kühling/Buchner/*Klar*, § 1 BDSG Rz. 29 ff.
13 HWK/*Lembke*, Einl. DSGVO Rz. 20.
14 Simitis/*Hansen*, Art. 4 Nr. 5 DSGVO Rz. 23.

wendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

18 Eine Datenverarbeitung fällt nur dann in den Anwendungsbereich der DSGVO, wenn sie zumindest teilweise **automatisiert** erfolgt oder sich auf personenbezogene Daten bezieht, die in einem **Dateisystem** gespeichert werden sollen oder dies bereits sind (Art. 2 Abs. 1 DSGVO). Beide Fallgruppen sind sehr weit zu verstehen: Der Begriff der Automatisierung erfasst jeden Einsatz von Datenverarbeitungsanlagen[15]. Ein Dateisystem ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird (Art. 4 Nr. 6 DSGVO). Damit werden nahezu sämtliche elektronisch gespeicherten personenbezogenen Daten durch die DSGVO erfasst[16]. Die **Personalakte** unterliegt ohnehin dem Anwendungsbereich der DSGVO, wenn sie in elektronischer Form geführt wird. Papierakten fallen nach ErwGr 15 Satz 3 DSGVO zwar nur dann in den Anwendungsbereich der DSGVO, wenn sie nach bestimmten Kriterien geordnet sind. Dies ist jedoch bereits der Fall, wenn sie nach Personen sortiert sind, sodass auch die Papier-Personalakte idR von Art. 4 Nr. 6 DSGVO erfasst ist[17].

Der Anwendungsbereich des § 26 BDSG fällt weiter aus als jener der DSGVO (vgl. § 26 Abs. 7 BDSG). Die Norm erfasst sämtliche Verarbeitungen von Beschäftigtendaten, unabhängig davon, ob diese automatisiert und mittels Dateisystemen erfolgt (dazu Rz. 61 ff.).

c) Verantwortlicher

19 „Verantwortlicher" ist jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DSGVO). Unter der DSGVO ist nicht erforderlich, dass diese Stelle eine natürliche oder juristische Person ist[18]. Umstritten war bis zur Einführung des § 79a BetrVG durch das Betriebsrätemodernisierungsgesetz[19] vom 14.6.2021 deshalb, ob der Betriebsrat eigenständiger Verantwortlicher[20] oder bloß unselbständiger Teil des datenschutzrechtlich verantwortlichen Arbeitgebers ist (vgl. Rz. 123 ff.).

20 Legen zwei oder mehrere Verantwortliche gemeinsam die Zwecke und Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche** (Art. 26 Abs. 1 Satz 1 DSGVO). Voraussetzung ist, dass alle Beteiligten bei der Festlegung dieser Zwecke zu einem maßgeblichen Teil mitentscheiden[21]. Besteht für mehrere Konzernunternehmen innerhalb des Konzerns eine einheitliche Personalabteilung, verarbeiten die Konzernunternehmen die Beschäftigtendaten idR als gemeinsam Verantwortliche nach Art. 26 DSGVO (eingehend zur gemeinsamen Verantwortlichkeit von Konzernunternehmen Rz. 280 ff.)[22]. Gemeinsam Verantwortliche müssen in einer transparenten **Vereinbarung** festlegen, wer von ihnen welche datenschutzrechtlichen Verpflichtungen erfüllt (Art. 26 Abs. 1 Satz 2, 3 und Abs. 2 DSGVO). Zwar verlangt Art. 26 DSGVO nicht, dass diese in einer bestimmten Form geschlossen wird, allerdings empfiehlt der Europäische Datenschutzausschuss (**EDSA**), die Vereinbarung in Form eines **verbindlichen Dokuments** zu fassen[23].

---

15 Kühling/Buchner/*Kühling*/*Raab*, Art. 2 DSGVO Rz. 14; Paal/Pauly/*Ernst*, Art. 2 DSGVO Rz. 5, 6.
16 Plath/*Plath*, Art. 2 DSGVO Rz. 7; Ehmann/Selmayr/*Zerdick*, Art. 2 DSGVO Rz. 3.
17 LAG Sa.-Anh. v. 23.11.2018 – 5 Sa 7/17, NZA-RR 2019, 355 (356); *Herberger*, NZA 2020, 1665 (1667).
18 *Kort*, ZD 2017, 319 (323); *Wybitul*, NZA 2017, 413 (414); Simitis/*Petri*/*Stief*, Art. 4 Nr. 7 Rz. 16.
19 BGBl. I 2021, 1762.
20 So ua. LBfDI Baden-Württemberg: Der Ratgeber – Beschäftigtendatenschutz, S. 56 mwN zum Streitstand.
21 *Schreiber*, ZD 2019, 55; LBfDI Baden-Württemberg: Der Ratgeber – Beschäftigtendatenschutz, S. 40; Kühling/Buchner/*Hartung*, Art. 26 DSGVO Rz. 12.
22 Kühling/Buchner/*Hartung*, Art. 26 DSGVO Rz. 24.
23 Gola/Heckmann/*Piltz*, Art. 26 DSGVO Rz. 25.

Hinweis: 21
Das Institut der gemeinsamen Verantwortlichkeit wurde durch die DSGVO neu eingeführt. Die zuvor in Deutschland gebräuchliche sog. „**Funktionsübertragung**" ist seither rechtlich überholt[24]. Sie kann nicht mehr eingesetzt werden.

d) Auftragsverarbeiter

Vom gemeinsam Verantwortlichen ist der **Auftragsverarbeiter** abzugrenzen. Auftragsverarbeiter ist 22
eine fremde Stelle, die Daten im Auftrag, dh. auf Weisung[25] des Verantwortlichen, verarbeitet (Art. 28 Abs. 1 DSGVO). Dabei müssen sich die Weisungen des Verantwortlichen auf die Datenverarbeitungstätigkeit selbst beziehen, die idR (anders als bei sonstigen Subunternehmern) als Hauptleistung im Mittelpunkt der Vertragsbeziehung steht[26]. Anders als ein gemeinsam Verantwortlicher entscheidet der Auftragsverarbeiter bei der Festlegung der Zwecke der Datenverarbeitung nicht maßgeblich mit, sondern führt lediglich Weisungen des verantwortlichen Auftraggebers aus. Lässt ein Arbeitgeber **Personaldaten** durch einen Auftragsverarbeiter verarbeiten – etwa zur Entgeltabrechnung[27] –, bleibt er „Herr der Daten" und Verantwortlicher iSd. Art. 4 Nr. 7 DSGVO. Er ist damit für die Einhaltung der Datenschutzvorschriften durch den Auftragsverarbeiter verantwortlich (vgl. Art. 24 DSGVO). Das gilt auch bei der Nutzung konzerneigener „Shared Service Center" (SSC) für die Entgeltabrechnung[28].

Der Verantwortliche und der Aufragsverarbeiter müssen ihre Beziehung durch einen schriftlichen 23
(Art. 28 Abs. 9 DSGVO) Vertrag regeln, in dem sich der Auftraggeber den in Art. 28 Abs. 3 DSGVO enumerativ aufgeführten Garantien und Ansprüchen des Verantwortlichen unterwirft.

e) Dritter

Dritter ist jede gegenüber dem Verantwortlichen selbständige Stelle, die weder gemeinsam Verant- 24
wortlicher noch Auftragsverarbeiter ist (vgl. Art. 4 Nr. 10 DSGVO). Ein Dritter verarbeitet personenbezogene Daten nach Zwecken und mit Mitteln, die er eigenständig und ohne Abstimmung mit dem Verantwortlichen festlegt. Wenn der Verantwortliche personenbezogene Daten an einen Dritten übermittelt, entäußert er sich also seiner Herrschaftsmacht über diese personenbezogenen Daten. Bei der Datenübermittlung an Dritte bestehen deshalb erhöhte Anforderungen.

II. Organisationsaufgaben des Verantwortlichen

1. Verantwortlicher als Pflichtenadressat

Das Datenschutzrecht erschöpft sich nicht in Verbotsregeln, sondern gibt dem Arbeitgeber als Verant- 25
wortlichem eine Vielzahl von Handlungs- und Organisationsvorgaben auf. Unternehmen müssen aktiv tätig werden, um die **Datenverarbeitungsvorgänge** in ihrem Verantwortungs- und Herrschaftsbereich **nach einem rechtskonformen Gesamtkonzept zu strukturieren**.

Adressat der datenschutzrechtlichen Organisations- und Handlungspflichten ist der Verantwortliche 26
nach Art. 4 Nr. 7 DSGVO (dazu Rz. 19 ff.). Der Begriff des Verantwortlichen bestimmt zum einen,

24 *Schreiber*, ZD 2019, 55 (56).
25 Ehmann/Selmayr/*Bertermann*/*Peintinger*, Art. 28 DSGVO Rz. 3; BeckOK Datenschutzrecht/*Spoerr*, Art. 28 DSGVO Rz. 18.
26 Paal/Pauly/*Martini*, Art. 28 DSGVO Rz. 7.
27 Dazu *Maschmann*, BB 2019, 628 (631) mwN.
28 *Maschmann*, BB 2019, 628 (632) mwN; zur Haftung *Schlemann*, DB 2025, 307 ff.

welche Stelle die datenschutzrechtlichen Organisationspflichten erfüllen muss[29]. Zum anderen legt der Begriff der Verantwortlichen fest, auf welche Datenverarbeitungsvorgänge sich diese datenschutzrechtlichen Pflichten beziehen, nämlich sämtliche Datenverarbeitungsvorgänge, die dem Herrschaftsbereich des Verantwortlichen deshalb zuzurechnen sind, weil sie seinem tatsächlichen Einfluss unterliegen[30].

2. Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)

27 Beschäftigt der Verantwortliche 250 oder mehr Mitarbeiter (Art. 30 Abs. 5 DSGVO)[31], muss er sämtliche Datenverarbeitungstätigkeiten, die er praktiziert, in einem schriftlich zu führenden **Verzeichnis aller Verarbeitungstätigkeiten** tabellarisch dokumentieren (Art. 30 Abs. 1 DSGVO). Dabei sind zu jeder Verarbeitungstätigkeit die in Art. 30 Abs. 1 Satz 2 DSGVO enumerativ aufgeführten Angaben aufzunehmen, namentlich Zwecke, betroffene Personen, Datenkategorien, Empfängerkategorien, Löschfristen, etwaige Schutzmaßnahmen und eine etwaige Übermittlung in das Ausland.

Das Verzeichnis der Verarbeitungstätigkeiten ist als Ausgangspunkt jeder datenschutzrechtlichen **Überprüfung durch Datenschutzbehörden** gedacht (ErwGr 82 DSGVO)[32]. Fehlen in der Dokumentation wesentliche Verarbeitungstätigkeiten, liegt darin ein gewichtiger Verstoß gegen die DSGVO.

28 Sämtliche praktizierten und somit im Verzeichnis der Verarbeitungstätigkeiten dokumentierten Datenverarbeitungstätigkeiten müssen materiellrechtlich zulässig sein (dazu Rz. 51). Anlässlich der Zusammenstellung des Verzeichnisses der Verarbeitungstätigkeiten sollten Unternehmen also die **Rechtmäßigkeit sämtlicher Datenverarbeitungstätigkeiten hinterfragen** und einzelne Verarbeitungsvorgänge nötigenfalls anpassen oder ganz einstellen.

3. Informationspflichten (Art. 13, 14 DSGVO)

29 Gemäß Art. 13, 14 DSGVO müssen alle betroffenen Personen über Verarbeitungstätigkeiten informiert werden, die ihre personenbezogenen Daten betreffen. Im Bereich des Beschäftigtendatenschutzes handelt es sich um alle Mitarbeiter des Unternehmens (**Arbeitnehmer**, **Auszubildende**, **Praktikanten**) sowie sämtliche **Bewerber** (vgl. auch § 26 Abs. 8 BDSG).

30 Die Information muss vor oder (spätestens) bei Erhebung der personenbezogenen Daten erfolgen[33], dh. spätestens ab Aufnahme der Arbeitstätigkeit. Es ist nicht praktikabel, bei jedem Datenerhebungsvorgang gesondert zu informieren. Stattdessen empfiehlt es sich für Arbeitgeber, umfassende Informationsschreiben zu erstellen, welche die nach Art. 13, 14 DSGVO vorgeschriebenen Informationspflichten **vorab** für sämtliche Datenverarbeitungsvorgänge erfüllen, die im Verlauf des Beschäftigungsverhältnisses in Betracht kommen[34]. Diese Informationsschreiben sollte der Arbeitgeber an neu einzustellende Arbeitnehmer als „**Beipackzettel**“[35] **zum Arbeitsvertrag** übergeben und an die Altbelegschaft in alljährlich aktua-

29 Kühling/Buchner/*Hartung*, Art. 4 Nr. 7 DSGVO Rz. 6; Simitis/*Petri*/*Stief*, Art. 4 Nr. 7 DSGVO Rz. 20; BeckOK Datenschutzrecht/*Schild*, Art. 4 DSGVO Rz. 88.

30 BeckOK Datenschutzrecht/*Schild*, Art. 4 DSGVO Rz. 93a f.

31 Die Verpflichtung soll auch für kleinere Unternehmen bereits dann gelten, wenn sie besondere Kategorien personenbezogener Daten iSd. Art. 9 DSGVO verbarbeiten (Art. 30 Abs. 5 Halbs. 2 DSGVO). Dies wäre aber streng genommen bei jedem Unternehmen der Fall, da im Zusammenhang mit der Abführung der Kirchensteuer durch die Lohnbuchung stets personenbezogene Daten verarbeitet werden, aus denen die religiöse Überzeugung hervorgeht.

32 Kühling/Buchner/*Hartung*, Art. 30 DSGVO Rz. 12.

33 BeckOK Datenschutzrecht/*Schmidt-Wudy*, Art. 13 DSGVO Rz. 79; Kühling/Buchner/*Bäcker*, Art. 13 DSGVO Rz. 78.

34 Kritisch zur Information „auf Vorrat“ jedoch Gola/Heckmann/*Franck*, Art. 13 DSGVO Rz. 12.

35 Begriff nach *Kamps*/*Bonanni*, ArbRB 2017, 119 (122).

lisierten Fassungen als Rundmail[36] übermitteln. Für den Bewerbungsprozess müssen gesonderte Unterrichtungsschreiben erstellt werden (zum Bewerbungsprozess Rz. 198 ff.).

Welche Informationspflichten bei der **Konzerndatenübermittlung** bestehen, hängt entscheidend davon ab, ob sich die Konzernunternehmen als gemeinsam Verantwortliche iSd. Art. 26 DSGVO oder als Dritte gegenüberstehen (dazu Rz. 280 ff.). 31

Wie detailliert die Information erfolgen muss, ist bislang noch ungeklärt. Die derzeit überwiegende Auffassung in der Literatur verlangt vollständige und so **detaillierte Angaben**, dass sich der betroffene Mitarbeiter ein Bild machen kann, mit welchen Datenverwendungen zu rechnen ist[37]. Nur eine Mindermeinung hält formelhafte Wendungen für ausreichend[38]. Will der Arbeitgeber den sicheren Weg gehen, sollte er das Informationsschreiben anhand seines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO formulieren und für jeden dort aufgeführten Datenverarbeitungsprozess, der Beschäftigtendaten betrifft, Datenkategorien, Zweck, Rechtsgrundlage, Mitteilungspflichten bzw. Quellen, Empfänger und Löschfrist benennen[39]. 32

Im Informationsschreiben müssen die Beschäftigten außerdem über ihre Rechte nach Art. 15 ff. DSGVO belehrt werden.

Hinweis: 33
Die Weiterleitung von Beschäftigtendaten an einen **Rechtsanwalt** im Rahmen eines arbeitsrechtlichen Mandats ist nach § 33 Abs. 2 Nr. 2 lit. a BDSG iVm. § 23 Abs. 1 lit. i DSGVO gegenüber der betroffenen Person idR nicht informationspflichtig.

4. Löschpflichten (Art. 17 DSGVO)

Das „**Recht auf Vergessenwerden**" war eines der zentralen Motive für die Schaffung der DSGVO. Besteht kein hinreichender Aufbewahrungsanlass, muss der **Verantwortliche** die personenbezogenen Daten nach Art. 17 Abs. 1 DSGVO **von sich aus löschen**, dh. unabhängig davon, ob der Betroffene einen Löschungsanspruch geltend gemacht hat oder nicht[40]. Um dieser Pflicht gerecht zu werden, ist es unerlässlich, dass Verantwortliche **Löschkonzepte** mit **standardisierten Löschfristen** entwerfen und auf deren Grundlage **automatisierte Löschroutinen** für elektronisch gespeicherte personenbezogene Daten implementieren (vgl. auch Art. 5 Abs. 1 lit. e DSGVO)[41]. Arbeitgeber, die ihre Akten elektronisch führen, sind dabei im Vorteil. 34

Hinweis: 35
Datenschutzrechtlich sind Unternehmen ohnehin verpflichtet, die Löschpflicht des Art. 17 DSGVO für alle personenbezogenen Daten zu beachten, nicht nur bei Beschäftigtendaten. Insoweit lässt sich die Löschpflicht bezüglich Personaldaten auf der Grundlage des allgemeinen unternehmensweiten Löschkonzepts technisch bei der jeweils verwandten Software implementieren. Eine „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten" enthält DIN 66398 (Stand Mai 2016).

Der von der Rspr. entwickelte Anspruch auf Entfernung einer **Abmahnung** nach §§ 242, 1004 BGB analog konkurriert hinsichtlich der Anspruchsgrundlagen aus Art. 17 Abs. 1 lit. a DSGVO (Zeitablauf bzw. Aus-

36 Nach Art. 12 Abs. 1 Satz 2 DSGVO kann die Übermittlung „gegebenenfalls auch elektronisch" erfolgen.

37 Kühling/Buchner/*Bäcker*, Art. 13 DSGVO Rz. 25; Sydow/*Ingold*, Art. 13 Rz. 15; Gola/Heckmann/*Franck*, Art. 13 DSGVO Rz. 12.

38 So Schaffland/Wiltfang/*Schaffland*/*Holthaus*, Art. 13 Rz. 11; „Schlagworte" sollen ausreichen nach Plath/*Kamlah*, Art. 13 DSGVO Rz. 11.

39 Ausführliches Muster bei *Grimm*/*Kühne*, ArbRB 2018, 185.

40 Plath/*Kamlah*, Art. 17 DSGVO Rz. 6; Paal/Pauly/*Paal*, Art. 17 DSGVO Rz. 20: Gola/Heckmann/*Nolte*/*Werkmeister*, Art. 17 DSGVO Rz. 9; kritisch Kühling/Buchner/*Herbst*, Art. 17 DSGVO Rz. 8 ff.

41 So auch *Dzida*, BB 2018, 2677 (2680).

scheiden aus dem Unternehmen[42]) bzw. Art. 17 Abs. 1 lit. d DSGVO (unrechtmäßige Datenverarbeitung, was bei einer rechtswidrigen Abmahnung der Fall ist) mit dem Löschungsanspruch gem. Art. 17 DSGVO. Die Rechtsfolgen können aber deutlich intensiver sein: Einmal ist dies der Schadensersatzanspruch nach Art. 82 Abs. 1 DSGVO und zum anderen die Bußgeldsanktionierung nach Art. 83 Abs. 5 lit. b DSGVO[43].

36 Die Löschfristen müssen sowohl im Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 1 Satz 2 lit. f DSGVO) als auch in der Datenschutzinformation an die Belegschaft (Art. 13 Abs. 2 lit. a, Art. 14 Abs. 2 lit. a DSGVO) angegeben werden. Unternehmen sollten darauf achten, dass sich die Angaben nicht widersprechen.

37 Wie lange die Löschfristen maximal bemessen werden dürfen, richtet sich nach Art. 17 Abs. 1 und Abs. 3 DSGVO. Löschfristen bestehen nicht erst nach Beendigung des Arbeitsverhältnisses, sondern auch schon im laufenden Arbeitsverhältnis[44].

38 **Hinweis:**
Bewerberdaten sind nach Erfüllung des Zwecks – Durchführung des Bewerbungsverfahrens – zu löschen. Eine über sechs Monate dauernde Speicherung dürfte unzulässig sein, weil diese dann nicht mehr zur Verteidigung von Rechtsansprüchen des Arbeitgebers (Art. 17 Abs. 3 lit. 3 DSGVO) gegen Diskriminierungsklagen notwendig ist. Der Diskriminierte hat zwei Monate Zeit zur schriftlichen Geltendmachung der Ansprüche nach Zugang der Ablehnungsentscheidung (§ 15 Abs. 4 AGG) und weitere drei Monate zur Klageerhebung (§ 61b Abs. 1 ArbGG). Unter Berücksichtigung eines Zugangszeitraums der Klage von einem Monat dürften **sechs** Monate Speicherdauer genügend sein[45]. Will der Arbeitgeber die Daten länger – etwa für einen Stellenpool und bei Initiativbewerbungen – verwenden, bedarf es der (informierten) Einwilligung des Bewerbers nach § 26 Abs. 2 BDSG.

39 Die Beendigung des Arbeitsverhältnisses erzwingt nicht bei sämtlichen Beschäftigtendaten die Löschung. Zwar sind die Beschäftigtendaten bei Ausscheiden des Arbeitnehmers idR nicht mehr für denjenigen Zweck notwendig, für den sie ursprünglich erhoben wurden (vgl. Art. 17 Abs. 1 lit. a DSGVO). Allerdings dürfen Beschäftigtendaten nach Art. 17 Abs. 3 lit. a und lit. e DSGVO weiterhin gespeichert werden, wenn hierzu eine **öffentlich-rechtliche Verpflichtung** besteht oder, wenn sie noch für eine etwaige **Verteidigung gegen Rechtsansprüche** erforderlich werden könnten. Öffentlich-rechtliche Aufbewahrungspflichten ergeben sich vor allem aus § 147 AO, § 257 HGB und § 28f SGB IV. Zur Verteidigung gegen Rechtsansprüche ist die Aufbewahrung von Unterlagen insbesondere dann erforderlich, wenn aus dem Beschäftigungsverhältnis prinzipiell Klagen drohen. Da automatisierte Löschroutinen nur **generalisiert** eingerichtet werden können, muss der Arbeitgeber das Klagerisiko ebenso abstrakt generalisiert bewerten[46]. Dazu bietet sich eine Orientierung an den arbeitsvertraglichen Verjährungsfristen an.

40 **Hinweis:**
Die Löschung muss ohne Rückholmöglichkeit erfolgen. Da einmal gelöschte personenbezogene Daten unwiederbringlich verloren sind, muss dringend davor gewarnt werden, Löschfristen zu kurz zu bemessen.

Beschäftigtendaten[47] sollten erst dann gelöscht werden, wenn die **Verjährungsfristen** für alle denkbaren Ansprüche des Arbeitnehmers abgelaufen sind, für deren Prüfung und Abwehr die Beschäftigtendaten ggf.

---

42 Dazu LAG Sa.-Anh. v. 23.11.2018 – 5 Sa 7/17, NZA-RR 2019, 355 (356).
43 Eingehend *Herberger*, NZA 2020, 1665 (1668 f.), die auf die Beobachtungspflicht des Arbeitgebers zur Entfernung „zu alter" oder unrechtmäßiger Abmahnungen hinweist und eine Abmahnungs-Compliance-Organisation anregt.
44 *Dzida*, BB 2018, 2677 (2680).
45 Kühling/Buchner/*Maschmann*, § 26 BDSG Rz. 28; BayLDA RDV 2013, 141 f.; aA LBfDI Baden-Württemberg: Der Ratgeber – Beschäftigtendatenschutz, S. 32: vier Monate.
46 Zu Unrecht zweifelnd Kühling/Buchner/*Maschmann*, § 26 BDSG Rz. 56; wie hier *Dzida*, BB 2018, 2677 (2680); Plath/*Kamlah*, Art. 17 DSGVO Rz. 6 u. 20.
47 Eine Übersicht über mögliche Löschfristen für die verschiedenen Kategorien von Beschäftigtendaten geben *Grimm*/*Kühne*, ArbRB 2018, 144; zustimmend *Dzida*, BB 2018, 2677 (2681). Zu Speicherdauer

noch erforderlich werden könnten. Arbeitsvertragliche Ansprüche verjähren grundsätzlich innerhalb der regelmäßigen Verjährungsfrist, dh. drei Jahre nach Schluss des Jahres der Anspruchsentstehung (§§ 195, 199 Abs. 1 BGB). Sollte allerdings eine betriebliche Altersversorgung bestehen, muss für die insoweit relevanten Unterlagen eine deutlich längere Verjährungsfrist beachtet werden (vgl. § 18a BetrAVG).

Die Information, dass eine bestimmte Person sich als Arbeitnehmer in einem Beschäftigungsverhältnis mit dem eigenen Unternehmen befunden hat, sollte im Hinblick auf das **Vorbeschäftigungsverbot** nach § 14 Abs. 2 Satz 2 TzBfG wenigstens zwanzig Jahre aufbewahrt werden[48], was wegen der sonst drohenden Unwirksamkeit einer sachgrundlosen Befristung gerechtfertigt erscheint.

Speichert der Arbeitgeber personenbezogene Daten unter Verletzung von Löschpflichten zu lange, ergibt sich kein prozessuales Beweisverwertungsverbot in Hinblick auf die unzulässig besessenen Daten. Die personenbezogenen Daten können gleichwohl als Sachvortrag und Beweismittel in einen Prozess eingeführt werden[49]. 41

5. Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Nach Art. 35 Abs. 1 DSGVO muss der datenschutzrechtlich verantwortliche **Arbeitgeber** eine **Datenschutz-Folgenabschätzung vornehmen**, wenn infolge einer von ihm verwendeten Form der Datenverarbeitung für die „Rechte und Freiheiten" natürlicher Personen ein hohes Risiko besteht. Dies kann zB aufgrund der Verwendung neuartiger Technologien der Fall sein. Auch derart eingriffsintensive Formen der Datenverarbeitung können zulässig sein, wenn sie in ihrer konkreten Ausgestaltung durch ausreichend gewichtige Interessen des verarbeitenden Unternehmens gerechtfertigt sind (dazu Rz. 65 ff.). Dabei drohen allerdings Bußgelder, wenn die Datenschutz-Folgenabschätzung vor der Einführung der Technik nicht vorgenommen wurde (Art. 83 Abs. 4 lit. a DSGVO). 42

Die Datenschutz-Folgenabschätzung ist eine **mehrstufige Prüfung**, bei welcher die geplanten Verarbeitungsvorgänge inhaltlich beschrieben, ihre Notwendigkeit sowie ihre Risiken bewertet und für erkannte Risiken Abhilfemaßnahmen entworfen werden (Art. 35 Abs. 7 DSGVO). Sämtliche Prüfungsschritte sind schriftlich zu dokumentieren[50]. Arbeitgeber müssen den Datenschutzbehörden entsprechende Dokumentationen vorlegen können, wenn sie datenschutz-folgenabschätzungspflichtige Datenverarbeitungsvorgänge praktizieren. 43

Auf Grundlage von Art. 35 Abs. 4 DSGVO haben sämtliche deutschen Datenschutzbehörden übereinstimmende **Positiv-Listen** veröffentlicht, die (nicht abschließend) Fälle aufzählen, in denen sie eine Datenschutz-Folgenabschätzung für erforderlich halten[51]. Im Bereich des Beschäftigtendatenschutzes beachtlich sind

- **automatisierte Aufenthaltsbestimmungen** von Mitarbeitern, zB durch GPS-Tracking (dazu Rz. 293 ff.),
- **automatisiertes Scoring**, zB die automatisierte Bewertung der Leistung und des Entwicklungspotentials von Mitarbeitern anhand elektronisch erfasster Kennzahlen,
- **automatisierte Aufzeichnungen** von Aspekten des Arbeitsverhaltens **in derart großem Umfang**, dass sich hieraus Verhaltensprofile erstellen lassen, zB im Rahmen **eines „Data-Loss-Prevention"-Systems (DLP)**, und
- systematische Auswertung des Verhaltens der Mitarbeiter anhand von **Monitoring** und **Login-Daten**.

---

und Löschfristen auch *Haußmann*/*Karwatzki*/*Ernst*, DB 2018, 2697; *Faas*/*Henseler*, BB 2018, 2292. Zu Aufbewahrungsfristen für BEM-Unterlagen speziell *Anton-Dyck*/*Böhm*, ArbRB 2020, 280.

48 Folge von BAG v. 23.1.2019 – 7 AZR 733/16; BVerfG v. 6.6.2018 – 1 BvL 7/14, 1 BvR 1375/14, NZA 2018, 774.

49 BAG v. 23.8.2018 – 2 AZR 133/18, NZA 2018, 1329 Rz. 35.

50 Kühling/Buchner/*Jandt*, Art. 35 DSGVO Rz. 51.

51 Vgl. Kühling/Buchner/*Kühling*/*Sackmann*, § 38 BDSG Rz. 11.

Stellt das Unternehmen bei der Datenschutz-Folgenabschätzung ein hohes Risiko fest, muss es nach Art. 36 DSGVO die **Datenschutzbehörde konsultieren**, bevor es die Datenverarbeitung einführt.

44 **Hinweis:**
Die Einführung von Personaldatenverarbeitungsverfahren, die datenschutz-folgenabschätzungspflichtig ist, ist fast immer gem. Art. 87 Abs. 1 Nr. 6 BetrVG mitbestimmt. Es empfiehlt sich deshalb, die **Verhandlungen mit dem Betriebsrat** in der Form einer Datenschutz-Folgenabschätzung zu führen. IdR setzen sich die Betriebsparteien in ihren Verhandlungen nämlich ohnehin mit denselben Fragen auseinander, die bei der Datenschutz-Folgenabschätzung geprüft werden (vgl. Art. 35 Abs. 7 DSGVO). Wird dieser Prüfungsprozess angemessen dokumentiert, lassen sich die Vorgaben des Art. 35 DSGVO gleich miterfüllen. Dies gibt auch dem Verhandlungsprozess eine geordnete Struktur.

6. Datenschutzbeauftragter (Art. 37–39 DSGVO)

45 Nicht öffentliche Stellen, die idR mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, müssen in Deutschland einen Datenschutzbeauftragten bestellen (§ 38 BDSG iVm. Art. 37 Abs. 4 DSGVO). Da der Begriff der automatisierten Verarbeitung weit gefasst ist (Rz. 17 f.), betrifft dies alle Unternehmen mit mindestens 20 Büroarbeitsplätzen[52].

46 Der Datenschutzbeauftragte steht als Instrument der **Selbstkontrolle** des Unternehmens neben der Fremdkontrolle durch die Aufsichtsbehörde. Der Datenschutzbeauftragte kann Beschäftigter des Unternehmens sein (sog. **„interner Datenschutzbeauftragter"**) oder aufgrund eines Dienstvertrages (sog. **„externer Datenschutzbeauftragter"**) tätig werden (Art. 37 Abs. 6 DSGVO). Er muss die zur Erfüllung seiner Aufgaben erforderliche **Fachkunde** und **Zuverlässigkeit** besitzen (Art. 37 Abs. 4 DSGVO). Dies sind **Kenntnisse** im Datenschutzrecht, hinreichende Kenntnis über die **Techniken** der Datenverarbeitung und Verständnis der betrieblichen **Abläufe**[53]. Er kann auch nebenamtlich tätig sein. Das Amt des Datenschutzbeauftragten und das des **Betriebsratsvorsitzenden** können nach Ansicht des BAG **nicht** durch dieselbe Person ausgeübt werden, da ein unauflösbarer Interessenkonflikt besteht[54]. Ob dies auch für die weiteren **Betriebsratsmitglieder** gilt, hat das BAG offengelassen[55]. Für eine Unvereinbarkeit der Ämter spricht, dass jedes Betriebsratsmitglied gleichwertig über die Verarbeitung der Daten mitbestimmt, § 33 Abs. 1 Satz 1 BetrVG. Da die Tätigkeit des Betriebsrats vom Datenschutzbeauftragten kontrolliert wird, müsste das Betriebsratsmitglied, das gleichzeitig Datenschutzbeauftragter ist, seinen eigenen Beschluss überwachen[56].

47 Wird ein bisher im Unternehmen beschäftigter Arbeitnehmer bestellt, liegt eine **Versetzung** iSd. § 95 Abs. 3 BetrVG vor. Der Betriebsrat kann bei fehlender Fachkunde und Zuverlässigkeit der Bestellung nach § 99 Abs. 2 Nr. 1 BetrVG **widersprechen**[57]. Die Bestellung des externen oder internen Datenschutzbeauftragten kann (nur) widerrufen werden, wenn ein wichtiger Grund für den Widerruf iSd. § 626 BGB gegeben ist (§ 38 Abs. 2 BDSG iVm. § 6 Abs. 4 Satz 1 BDSG)[58]. Die wichtigen Gründe müssen sich aus der Funktion oder Tätigkeit (zB Unzuverlässigkeit) ergeben. Das Arbeitsverhältnis des betrieblichen Datenschutzbeauftragten kann während der Bestellung zum Datenschutzbeauftragten und innerhalb eines Jahres nach der Beendigung der Bestellung nur aus **wichtigem Grund** gem. § 626 BGB gekündigt werden (§ 38 Abs. 2 BDSG iVm. § 6 Abs. 4 Satz 2, 3 BDSG). Das gilt ab dem Zeitpunkt der formfreien[59] Benennung und somit auch während einer vereinbarten Probe-

52 BeckOK Datenschutzrecht/*Moos*, § 38 BDSG Rz. 7 ff.; Kühling/Buchner/*Kühling*/*Sackmann*, § 38 BDSG Rz. 11.
53 Simitis/*Drewes*, Art. 37 DSGVO Rz. 41 ff.
54 BAG v. 6.6.2023 – 9 AZR 383/19, NZA 2023, 1329 Rz. 26 ff.
55 BAG v. 6.6.2023 – 9 AZR 383/19, NZA 2023, 1329 Rz. 26.
56 *Fitting*, § 79a BetrVG Rz. 60; *Brinkmann*, BB 2024, 54 (56 f.); *Dzida*/*Storms*, BB 2023, 2548 (2551).
57 BAG v. 11.11.1997 – 1 ABR 21/97, NZA 1998, 385 (387); DWWS/*Däubler*, Art. 37 DSGVO Rz. 20.
58 Zu den Kriterien HWK/*Lembke*, Art. 39 DSGVO Rz. 27 mwN.
59 Ehmann/Selmayr/*Heberlein*, Art. 37 DSGVO Rz. 17.

zeit[60]. Während der Dauer des Vertretungsfalls und für eine Nachwirkungsperiode von einem Jahr gilt der **Sonderkündigungsschutz** (vgl. dazu Teil 3 H Rz. 161 ff.)[61] auch für einen **stellvertretenden** Datenschutzbeauftragten[62]. Aufgrund eines Vorlagebeschlusses des BAG, ob die Regelung in § 38 Abs. 2 BDSG, § 6 Abs. 4 Satz 1 BDSG mit Art. 38 Abs. 3 Satz 2 DSGVO vereinbar ist[63], hat der EuGH entschieden, dass der Sonderkündigungsschutz des internen Datenschutzbeauftragten mit dem Unionsrecht vereinbar ist, solange die Ziele der DSGVO nicht gefährdet werden[64].

Die Entscheidung, zukünftig Datenschutzaufgaben durch einen externen Dritten wahrnehmen zu lassen, stellt auch in einer Konzernstruktur keinen Grund für die Abberufung des internen Datenschutzbeauftragten dar[65].

Hauptaufgabe ist gem. Art. 39 Abs. 1 lit. a DSGVO, auf die Einhaltung der DSGVO, des BDSG und anderer Datenschutzvorschriften hinzuwirken. Dazu kommt dem Datenschutzbeauftragten eine Kontrollfunktion zu (Art. 39 Abs. 1 lit. b DSGVO). Er ist in die Programmerstellung und Architektur des IT-Systems so frühzeitig einzuschalten, dass er noch eine Möglichkeit zur Einflussnahme hat (Art. 38 Abs. 1 DSGVO). Kraft Gesetzes übernimmt der Datenschutzbeauftragte die Sonderverantwortlichkeit für die Integrität des von ihm übernommenen Verantwortungsbereiches und hat eine **Garantenstellung** iSd. § 13 StGB inne[66]. 48

Hinweis: 49
Die Tätigkeit des **Betriebsrats** wurde früher nicht vom Datenschutzbeauftragten kontrolliert, weil dies mit der vom BetrVG vorgesehenen Unabhängigkeit des Betriebsrats vom Arbeitgeber als unvereinbar galt[67]. Mit der Einführung des § 79a BetrVG im Zuge des Betriebsrätemodernisierungsgesetzes[68] vom 14.6.2021 hat sich dies geändert. Der Gesetzgeber geht von der Zuständigkeit des betrieblichen Datenschutzbeauftragten für den Betriebsrat aus[69]. Neu sind darüber hinaus Vorschriften, die die Beziehung der Betriebsparteien und des Datenschutzbeauftragten zueinander regeln (§ 79a Satz 4 und 5 BetrVG). **§ 79a Satz 4 BetrVG** will verhindern, dass der unbegrenzte Zugang des Datenschutzbeauftragten zu allen Daten und Datenverarbeitungsvorgängen die Eigenständigkeit des Betriebsrats gefährdet und normiert deshalb eine Verschwiegenheitspflicht gegenüber dem Arbeitgeber für Informationen, die Rückschlüsse auf Meinungsbildungsprozesse im Betriebsrat zulassen[70]. **§ 79a Satz 5 BetrVG** enthält einen Verweis auf § 6 Abs. 5 Satz 2, § 38 Abs. 2 BDSG bezüglich des **Verhältnisses** des **Datenschutzbeauftragten** zum **Arbeitgeber**. Datenschutzbeauftragte werden dadurch verpflichtet, über die Identität von Personen, die den Datenschutzbeauftragten nach § 6 Abs. 5 BDSG zu Rate ziehen, bzw. über Umstände, die Rückschlüsse auf diese Personen zulassen, gegenüber dem Arbeitgeber Stillschweigen zu bewahren.

7. Gewährleistung eines angemessenen Schutzniveaus (Art. 32 DSGVO)

Nach Art. 32 DSGVO muss der Verantwortliche geeignete technische und organisatorische Maßnahmen (sog. **TOM**) ergreifen, um Datenverarbeitungen, die gegen die DSGVO verstoßen, zu verhindern. 50

60 ArbG Dortmund v. 20.2.2013 – 10 Ca 4800/12, RDV 2013, 319; ErfK/*Franzen*, § 38 BDSG Rz. 10.
61 Überblick zum Schutz vor Benachteiligung, Abberufung und Kündigung *Greiner*/*Senk*, NZA 2020, 201 ff.
62 So das ArbG Hamburg v. 13.4.2016 – 27 Ca 486/15, NZA-RR 2016, 353.
63 BAG v. 30.7.2020 – 2 AZR 225/20 (A), ZD 2021, 51 (52).
64 EuGH v. 22.6.2022 – C-534/20, NZA 2022, 1111. Folgend BAG v. 25.8.2022 – 2 AZR 225/20, NZA 2022, 1457.
65 BAG v. 23.3.2011 – 10 AZR 562/09, NZA 2011, 1036.
66 Kühling/Buchner/*Bergt*/*Herbort*, Art. 37 DSGVO Rz. 55; *Wybitul*, ZD 2016, 203 (205); *Wybitul*/*von Gierke* BB 2017, 181 (182); aA *Lantwin*, ArbRAktuell 2017, 50.
67 So BAG v. 11.11.1997 – 1 ABR 21/97, NZA 1998, 385 (388); ausdrücklich unter der Geltung der DSGVO zustimmend *Gola*, Handbuch Beschäftigtendatenschutz, Rz. 1713.
68 BGBl. I 2021, 1762.
69 BT-Drucks. 19/28899, 22; ausf. BeckOGK-BetrVG/*Grimm*, § 79a BetrVG Rz. 50 ff.
70 Hierzu *Grimm*/*Vitt*, ArbRB 2021, 279 (281); ausf. BeckOGK-BetrVG/*Grimm*, § 79a BetrVG Rz. 1 ff.

In der Gesamtschau muss er unter verhältnismäßiger Abwägung mit den Implementierungskosten ein dem Risiko angemessenes Schutzniveau gewährleisten. Ziel ist es dabei, sowohl einem unbefugten Zugriff durch Außenstehende als auch der unbefugten Verarbeitung durch das eigene Personal des Verantwortlichen (Art. 32 Abs. 4 DSGVO) entgegenzuwirken. Um dies zu erreichen, sollten Unternehmen geeignete technische Maßnahmen der IT-Sicherheit[71] umsetzen, bauliche Zugangshindernisse schaffen[72] und ihre eigenen Mitarbeiter anhand von Datenschutzrichtlinien ordnungsgemäß anweisen und überwachen[73].

III. Materielle Voraussetzungen der Datenverarbeitung

1. Datenschutzrechtliche Grundsätze (Art. 5 Abs. 1 DSGVO)

51 Bei der Datenverarbeitung sind die datenschutzrechtlichen Grundsätze nach Art. 5 Abs. 1 DSGVO zu beachten. Sie haben **unmittelbare Geltung** als Pflichten[74].

Personenbezogene Daten sind **rechtmäßig**, nach **Treu und Glauben** und **transparent** zu verarbeiten (Art. 5 Abs. 1 lit. a DSGVO). Ihre Verwendung unterliegt der **Zweckbindung** (Art. 5 Abs. 1 lit. b DSGVO). Insbesondere die Menge der verarbeiteten Daten ist nach dem Grundsatz der **Datenminimierung** zu begrenzen (Art. 5 Abs. 1 lit. c DSGVO). Inhaltlich müssen erhobene Daten **richtig** sein (Art. 5 Abs. 1 lit. d DSGVO). Für erhobene Daten muss zudem eine zeitliche **Speicherbegrenzung** bestehen (Art. 5 Abs. 1 lit. e DSGVO). Nach den Grundsätzen der **Integrität und Vertraulichkeit** sind personenbezogene Daten zudem mit technischen und organisatorischen Maßnahmen gegen unbefugte Verarbeitung, Verlust und Zerstörung zu schützen (Art. 5 Abs. 1 lit. f DSGVO).

52 Eine grundsätzliche Pflicht, personenbezogene Daten vorrangig bei der betroffenen Person selbst zu erheben (sog. „**Direkterhebung**"), ist in der DSGVO nicht mehr ausdrücklich normiert (anders noch § 4 Abs. 2 BDSG aF). Da es für die betroffene Person allerdings idR transparenter (vgl. Art. 5 Abs. 1 lit. a DSGVO) ist, wenn personenbezogene Daten direkt von ihr bezogen werden, kann der Verantwortliche nach dem Grundsatz der Verhältnismäßigkeit zur Direkterhebung verpflichtet sein[75].

53 Der Verantwortliche – also idR der Arbeitgeber – ist für die Einhaltung sämtlicher Grundsätze gegenüber den Datenschutzbehörden **rechenschafts- und nachweispflichtig** (Art. 5 Abs. 2 DSGVO).

2. Präventives Verbot mit Erlaubnisvorbehalt (Art. 6 Abs. 1 DSGVO)

54 Jeder Datenverarbeitungsvorgang, der in den Anwendungsbereich der DSGVO fällt, unterliegt einer gesonderten Rechtmäßigkeitsbewertung. Dabei stellt Art. 6 DSGVO die Datenverarbeitung unter ein **präventives Verbot mit Erlaubnisvorbehalt**[76].

Eine Verarbeitung personenbezogener Daten, dh. insbesondere das Erheben, Speichern, Verändern, das Auslesen, das Abfragen, Verwenden und Übermitteln personenbezogener Daten, ist **nur** zulässig, soweit die DSGVO **selbst** (zB in Art. 6 DSGVO) oder eine **andere Rechtsvorschrift** (zB § 26 Abs. 1 BDSG) dies erlaubt oder anordnet oder der Betroffene wirksam **eingewilligt hat**. Die Zulässigkeit muss bezogen auf **jedes** personenbezogene Datum und alle **Phasen** der Datenverarbeitung festgestellt

71 Kühling/Buchner/*Jandt*, Art. 32 DSGVO Rz. 15, 16.
72 Paal/Pauly/*Martini*, Art. 32 DSGVO Rz. 29.
73 Kühling/Buchner/*Jandt*, § 32 DSGVO Rz. 38.
74 Kühling/Buchner/*Bucher/Petri*, Art. 5 DSGVO Rz. 1.
75 LBfDI Baden-Württemberg: Der Ratgeber – Beschäftigtendatenschutz, S. 30; BeckOK Datenschutzrecht/*Riesenhuber*, § 26 BDSG Rz. 68.
76 Kühling/Buchner/*Bucher/Petri*, Art. 6 DSGVO Rz. 11.