Vertrauenswürdige Informationstechnik für die journalistische Arbeit

Schutzansprüche von Journalisten

Stand: 11.03.2024

Karin Schuler
schuler@netzwerk-datenschutzexpertise.de
Kronprinzenstraße 76, 53173 Bonn
Thilo Weichert
weichert@netzwerk-datenschutzexpertise.de
Waisenhofstraße 41, 24103 Kiel
www.netzwerk-datenschutzexpertise.de

Inhalt

Medien erfüllen in unserer freiheitlichen Demokratie eine Korrektivfunktion in Hinblick auf staatliche Gewalten. Journalistische Arbeit setzt voraus, mit Informanten vertraulich kommunizieren und die Rechercheergebnisse vertraulich bearbeiten können. Kommen dabei informationstechnische Dienste zum Einsatz, so kann diese Vertraulichkeit gefährdet sein. Das Gutachten des Netzwerks Datenschutzexpertise untersucht, welche verfassungs-, medien- und arbeitsrechtlichen Möglichkeiten für Journalisten in Medienunternehmen bestehen, die beruflich nötige Vertraulichkeit durchzusetzen.

1 Das Berufsgeheimnis journalistisch tätiger Personen

Die Medienfreiheit, also die Presse- und Rundfunkfreiheit, ist konstituierend für unsere **freiheitlich-demokratische Grundordnung**. Medien haben für die demokratische Meinungsbildung eine zentrale Funktion. Sie wirken als Korrektiv zu den staatlichen Gewalten – Verwaltung, Parlament und Rechtsprechung. Um diese Funktion wahrnehmen zu können, müssen die Medien von staatlicher Gewalt unabhängig recherchieren und berichten können. Ihnen kommt die Funktion eines „Wachhunds“ zu.[1] Die Medienfreiheit ist für Personen in der Medienbranche und deren betriebliche Organisationen subjektives Freiheitsrecht und hat eine objektivrechtliche Bedeutung für die institutionelle Eigenständigkeit der Presse und des Rundfunks – von der Informationsbeschaffung bis hin zur Verbreitung der Nachrichten und Meinungen.[2] Dem dient das strafprozessuale Zeugnisverweigerungsrecht nach § 53 Abs. 1 Nr. 5 Strafprozessordnung (StPO), das hieran anknüpfende Beschlagnahmeverbot nach § 97 Abs. 5 StPO sowie das zivilprozessuale Zeugnisverweigerungsrecht nach § 383 Abs. 1 Nr. 5 Zivilprozessordnung (ZPO). Um ihrer Funktion gerecht werden zu können, bedürfen Journalisten eines Freiraums, in dem sie vor staatlicher Einmischung geschützt sind.

Journalistische Arbeit ist heute ohne die Nutzung digitaler Werkzeuge nicht mehr vorstellbar. Dabei kann die Technik einen wichtigen Beitrag zur Wahrung und Absicherung von Vertraulichkeit und Unabhängigkeit leisten. Ebenso ist es allerdings möglich, dass die eingesetzten digitalen Werkzeuge zu einer Beeinträchtigung von **Vertraulichkeit und Unabhängigkeit** führen. Dies ist insbesondere zu bedenken, wenn digitale Werkzeuge von privaten Dritten zur Verfügung gestellt werden. Angestellte Journalisten nutzen in der Regel die durch ihren Arbeitgeber zur Verfügung gestellte Technik. . Ihre Unabhängigkeit kann daher im Falle unzureichender Ausgestaltung eingesetzter Technik auch durch die eigene Redaktion oder durch private Dritte beeinträchtigt werden.

Im Folgenden wird erörtert, inwieweit Journalisten gegenüber ihrem Arbeitgeber bzw. ihrer Redaktion einen Anspruch darauf haben, dass sie mit der hierüber **bereitgestellten Informationstechnik** (IT) selbstbestimmt vertraulich arbeiten können und wie ein solcher Anspruch verfassungsrechtlich, einfachgesetzlich und vertraglich zu bewerten ist.

1.1 Grundrechte

Art. 5 Abs. 1 S. 2 Grundgesetz (GG) gewährleistet die Pressefreiheit und die Freiheit der Berichterstattung durch den Rundfunk. Dies soll Menschen ihr Recht auf freie Meinungsäußerung und freien Informationszugang in Bezug auf meinungsbildende Medien garantieren. Das Grundrecht auf **Medienfreiheit** (Presse- und Rundfunkfreiheit) wird entsprechend auch in Art. 11 Abs. 2 der EU-

[1] EGMR 02.05.2012 – Nr. 20240/08, NJW 2012, 1053; EGMR 04.02.2015 – Nr. 30162/19.
[2] BVerfG 12.03.2003 – 1 BvR 330/96 u. 348/99, NJW 2003, 1793 m.w.N.

Grundrechtecharta (GRCh) garantiert. Medienfreiheit dient der möglichst uneingeschränkten Beschaffung, Auswertung und Vermittlung von Informationen und Meinungen.

Die Medienfreiheit wird zudem in Art. 10 der Europäischen Menschenrechtskonvention (EMRK) gewährleistet, der sowohl in den Mitgliedstaaten der **Europäischen Union** (EU) als auch von der EU selbst zu beachten ist (Art. 52 Abs. 3 GRCh). Zwar hat die EU bisher keine Kompetenzen im Medienrecht. Angesichts der Wechselwirkungen, z.B. mit dem Datenschutzrecht oder dem Wettbewerbsrecht, ist Art. 11 GRCh gleichwohl von Relevanz.[3] Deshalb plant die EU auch ein Medienfreiheitsgesetz zu erlassen.[4] Materiell und hinsichtlich der Schranken besteht zwischen der europarechtlichen Medienfreiheit und der Presse- und Rundfunkfreiheit des GG ein Gleichklang.

Die Medienfreiheit schützt den gesamten Bereich **publizistischer Tätigkeit**, insbesondere die Beschaffung von Informationen, die Informationsquellen sowie die zwischen diesen erfolgende Kommunikation,[5] aber auch die journalistische Aufbereitung des journalistischen Stoffs bis hin zur Veröffentlichung.[6] Grundrechtsträger sind die Medieneinrichtungen (Presse- und Rundfunkeinrichtungen), Redaktionen und Journalisten.[7] Die Gewährleistungsbereiche der Presse- und der Rundfunkfreiheit schließen diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können.

Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse bzw. Rundfunk und den Informanten[8] einschließlich der Wahrung des Redaktionsgeheimnisses.[9] Das **Redaktionsgeheimnis** schützt nicht nur die räumliche Sphäre der Redaktion bzw. der Arbeitsplätze der Journalisten vor Durchsuchung und Beschlagnahmung. Es schützt auch vor digitaler bzw. telekommunikativer Ausforschung sowohl hinsichtlich der Inhalts- als auch der Verbindungs- bzw. Metadaten.[10]

Das Recht auf informationelle Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ist europarechtlich als **Grundrecht auf Datenschutz** (Art. 8 GRCh) gewährleistet. Es beinhaltet die Befugnis der einzelnen natürlichen Person, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen.[11] Im

[3] Knecht in Schwarze, EU-Kommentar, 4. Aufl. 2019, Art. 11 GRCh Rn. 11.
[4] Art. 114 AUV; EU-Kommission, Vorschlag eines Medienfreiheitsgesetzes, v. 16.09.2022, COM(2022) 457 final, S. 9.
[5] BVerfG 06.02.1979 - 2 BvR 154/78, NJW 1979, 1401.
[6] BVerfG 12.03.2003 – 1 BvR 330/96 u. 348/99, NJW 2003, 1793; BVerfG 27.02.2007 1 BvR 538/06, 2045/06, NJW 2007, 1118;
[7] Von der Decken in Schmidt-Bleibtreu, Grundgesetz Kommentar, 15. Aufl. 2022, Art. 5 Rn. 22; Schemmer in Epping/Hillgruber, Grundgesetz Kommentar, 3. Aufl. 2020, Art. 5 Rn. 39, 62 ff.; Kaiser in Dreier, Grundgesetz Kommentar Bd. I, 4. Aufl. 2023, Art. 5 I, II Rn. 109-115; Schmidt in Erfurter Kommentar zum Arbeitsrecht, 23. Aufl. 2023, 10 Art. 5 Rn. 59.
[8] BVerfG 12.03.2003 – 1 BvR 330/96 u. 348/99, NJW 2003, 1793; BVerfG 14.07.1999 – 1 BvR 2226/94, 2420/95, 2437/95, NJW 2000, 58 m.w.N.; Beater, Medienrecht, 2. Aufl. 2016, Rn. 1112 f. m.w.N.
[9] BVerfG 05.08.1966 - 1 BvR 586/62, 610/63 u. 512/64, NJW 1966, 1603; BVerfG 27.02.2007 1 BvR 538/06, 2045/06, NJW 2007, 1118; Schmidt in Erfurter Kommentar zum Arbeitsrecht (Fn. 7), 10 Art. 5 Rn. 54..
[10] BVerfG 12.03.2003 – 1 BvR 330/96 u. 348/99, NJW 2003, 1792 f.; Ladeur in Paschke/Berlit/Meyer, Gesamtes Medienrecht, 4. Aufl. 2021, 4 Rn. 24.
[11] BVerfG 15.112.1984 – 1 BvR 209/83 u.a., NJW 1984, 419 ff.

Kontext journalistischer Tätigkeit steht es dem Journalisten, dem Informanten und auch betroffenen Personen zu (also solchen, die Gegenstand einer Information sind).

Die Vertraulichkeit der Kommunikation anlässlich journalistischer Arbeit wird zudem in Art. 10 GG sowie in Art. 7 GRCh durch das Fernmeldegeheimnis bzw. das **Telekommunikationsgeheimnis** (TK-Geheimnis) geschützt. Die Medienfreiheit, der Datenschutz und das TK-Geheimnis verstärken und ergänzen sich gegenseitig, wenn es darum geht, die journalistische Vertraulichkeit zu wahren.

Nutzt ein Medienunternehmen für seine journalistische Tätigkeit einen informationstechnischen (IT-) **Dienstleister**, so wird die Entscheidung hierüber, unbeschadet evtl. bestehender Mitbestimmungsrechte einer Beschäftigtenvertretung, auch durch die Medienfreiheit sowie die Unternehmensfreiheit (Art. 16 GRCh) geschützt. Motiviert sind diese Entscheidungen durch das Streben nach größtmöglicher Wirtschaftlichkeit, Entlastung von berufsfremden Tätigkeiten sowie hoher Funktionalität. Dieses Interesse hat ein geringeres Gewicht als das grundrechtlich geschützte journalistische „Datengeheimnis“ bzw. das Redaktionsgeheimnis (s.u. I.4-I.6).

1.2 Grundrechtsschutz beim Hilfsunternehmen

Gemäß der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) erstreckt sich der Schutz der Medienfreiheit auch auf **Hilfstätigkeiten**, aber nur, soweit diese „notwendige Bedingung der Funktion einer freien Presse ist“.[12] Es bedarf eines „ausreichenden Inhaltsbezugs“[13], mindestens „um pressetechnische Hilfstätigkeiten, einschließlich der Tätigkeiten zur Erhaltung der wirtschaftlichen Grundlagen der Unabhängigkeit des Presseunternehmens als notwendige Voraussetzung einer freien Presse“.[14]

Dem folgend sieht das Medienrecht vor, dass sich die journalistische Vertraulichkeit auch auf die „Hilfsunternehmen“ erstreckt. Das Hilfsunternehmen darf nur zur Unterstützung des Journalisten bzw. der Redaktion tätig werden, mit erlangten Daten aber keine eigenen Zwecke verfolgen.

Medienexterne Hilfstätigkeiten unterfallen also nur ausnahmsweise dem Schutzbereich der Medienfreiheit, wenn sie typischerweise medienbezogen sind, in enger organisatorischer Bindung an die Medientätigkeit erfolgen und für dessen freies Funktionieren notwendig sind und sich ihre Beschränkung zugleich auf die Meinungswirkung auswirkt. Es muss ein spezifischer Bezug zur Medienarbeit bestehen. Inhaltsferne medientechnische Hilfstätigkeiten sind nicht durch die Medienfreiheit geschützt.[15]

Die Einschaltung von IT-Unternehmen bei der Vorbereitung, Herstellung oder Verbreitung von journalistischer Arbeit unterscheidet sich zumeist nicht von der Mitwirkung bei nicht privilegierten Kommunikations- und Datenverarbeitungsvorgängen. Bei den Aktivitäten etwa eines allgemeinen IT-Dienstleisters wie Microsoft handelt es sich daher nicht um „medientypischen Tätigkeiten“ i.S.v.

[12] BVerfG 25.01.1984 – 1 BvR 272/81, BVerfE 66, 134.
[13] BVerfG 13.01.1988 – 1 BvR 1548/82, BVerfGE 77, 346, 354.
[14] BVerfG 12.04.2007 – 1 BvR 78/02, NVwZ 2007, 1306.
[15] Kaiser in Dreier (Fn. 7), Art. 5 I, II, Rn. 90; Trute in Merten/Papier, Handbuch der Grundrechte IV Einzelgrundrechte I, 2011, § 104 Rn. 22 f.

„Hilfstätigkeiten“, die in Folge des fehlenden verfassungsrechtlichen Schutzes auch einfachgesetzlich nicht privilegiert sind.[16]

Etwas anderes gilt, wenn es sich bei der IT-Tätigkeit um eine **spezifische Hilfstätigkeit** für die journalistische Arbeit handelt. Zielt die IT-Hilfe vorrangig darauf ab, dass die journalistische Vertraulichkeit gewahrt wird, so nimmt diese am Grundrechtsschutz teil. Dabei muss die Wahrung der journalistischen Vertraulichkeit im Vordergrund stehen und sich durch spezifische Maßnahmen auszeichnen, die über allgemeine Schutzvorkehrungen der Datensicherheit hinausgehen.

1.3 Europarechtlicher Rahmen

Auf europäischer Ebene regelt Art. 85 Abs. 2 **Datenschutz-Grundverordnung** (DSGVO) die Verarbeitung personenbezogener Daten für journalistische Zwecke. Demgemäß „sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen“. Dieses datenschutzrechtliche „Medienprivileg“[17] stellt die Medien nicht von Datenschutzpflichten frei, sondern zielt darauf ab, ein Gleichgewicht bzw. einen Ausgleich zwischen freier Meinungsäußerung und dem Schutz der Privatsphäre herzustellen, soweit diese Grundrechte zueinander in einem Konflikt stehen.[18]

Die EU plant ein **Medienfreiheitsgesetz**. Ein Ziel dieser Gesetzgebung ist der Vertraulichkeitsschutz journalistischer Tätigkeit. Das Gesetz soll den Einsatz von Spähsoftware, die in Geräten von Medienanbietern eingesetzt werden, grundsätzlich verbieten.[19] Es macht aber keine Aussagen über das Verhältnis zwischen Medienanbietern, Journalisten und IT-Diensten. Streitig ist die Frage, inwieweit staatliche Einrichtungen befugt sein sollen, Spähsoftware für Sicherheitszwecke gegenüber Journalisten einzusetzen.[20]

1.4 Allgemeine nationale Regelungen

Der Schutz des **Zeugnisverweigerungsrechts** in Bezug auf Strafverfolgung nach § 53 Abs. 1 Nr. 5 StPO, die entsprechende Durchsuchungs- und Beschlagnahmeeinschränkung in § 97 Abs. 5 StPO sowie das zivilprozessuale Zeugnisverweigerungsrecht nach § 383 Abs. 1 Nr. 5 ZPO schützt Journalisten vor hoheitlichen Eingriffen. Vorgaben für den journalistischen IT-Einsatz sind damit nicht verbunden. Es ist fraglich, ob IT-Dienstleister für Redaktionen und Journalisten als „Mitwirkende“ hierüber einen spezifischen Schutz vor Beschlagnahme und eine Berechtigung zur Zeugnisverweigerung genießen. Ein solcher Schutz besteht nur für Mitwirkende von besonderen Berufsgeheimnisträgern nach § 203

[16] Rogall Systematischer Kommentar zur Strafprozessordnung (SK-StPO), Bd. I, 5. Aufl. 2018, § 53 Rn. 161 ff.; Weberling in Ricker/Weberling, Handbuch des Presserechts, 7. Aufl. 2021, 30. Kap. Rn. 23.
[17] Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 85 Rn. 21; Hennemann in Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 19 Rn. 38.
[18] EuGH 16.12.2008 – C-73/07Rn. 56, MMR 2009, 177; Dix in Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 85 Rn. 20, 22.
[19] EU-Kommission, Vorschlag eines Medienfreiheitsgesetzes (Fn. 4), ErwGr 6, Art. 4 Abs. 2 lit. c.
[20] Reporter ohne Grenzen, PE v. 11.12.2023, Vertrauliche Kommunikation schützen;

Strafgesetzbuch (StGB) bzw. § 53 Abs. 1 Nr. 1-4 StPO. Amtsträger werden auch durch § 203 Abs. 2 StGB verpflichtet, wozu gemäß der Rechtsprechung des Bundesgerichtshofs (BGH) auch Redakteure öffentlich-rechtlicher Rundfunkanstalten gehören.[21] Dass sich hieraus Pflichten für die Auswahl der IT-Anbieter ergeben, wurde bisher rechtlich nicht abgeleitet.

Einfachgesetzliche Regelungen, die Presse- und Rundfunkunternehmen sowie deren Journalisten spezifisch zur technischen Sicherstellung von Vertraulichkeit verpflichten, bestehen nicht. Die Wahrung der Vertraulichkeit unterliegt der Absprache mit Quellen und der Entscheidung der Redaktionen bzw. Journalisten. Durch die Informanten können allenfalls Haftungsansprüche wegen absprachewidriger Offenlegung erteilter Informationen geltend gemacht werden.[22]

Es gibt auch keine gesetzliche Regelung, die explizit einen **Anspruch der Journalisten** gegenüber seinem Arbeitgeber auf Unterstützung bei der Wahrung der Vertraulichkeit begründet. Wohl aber ist ein solcher Anspruch rechtlich abzuleiten. Dies wird im Folgenden dargelegt.

Hinsichtlich der Wahrung des Datenschutzes bei der Telekommunikation ist nicht die DSGVO anwendbar, sondern auf europäischer Ebene die Telekommunikations-Datenschutz-Richtlinie (ePrivacy-RL) sowie deren Umsetzung im **Telekommunikation-Telemedien-Datenschutzgesetz** (TTDSG).[23] Gegenüber dem Datenschutzrecht garantiert der gesetzliche Schutz des TK-Geheimnisses (§ 3 Abs. 1 TTDSG) einen erhöhten Schutz der Kommunikationsinhalte wie auch der Nutzungsdaten (Meta-Daten, „nähere Umstände der Telekommunikation“). Das TTDSG enthält keine spezifischen Regelungen zugunsten von journalistischen Medien. Die Anwendung der Regeln des TTDSG muss aber bei journalistischer Kommunikation im Lichte der Medienfreiheit erfolgen.

1.5 Presserecht

Die rechtlichen Rahmenbedingungen für die Pressearbeit werden in Deutschland durch die Pressegesetze definiert. Presserecht ist in der Kompetenzordnung des deutschen Grundgesetzes weitgehend **Ländersache**. In Landespressegesetzen finden sich allgemeine Regelungen zum „Medienprivileg“ bzw. zur „Datenverarbeitung zu journalistischen Zwecken“, mit denen eine teilweise Freistellung von datenschutzrechtlichen Pflichten einhergeht. Zugleich werden die Mitarbeiter des Arbeitgebers bzw. des Journalisten zu einer strengen Zweckbindung, einem „Datengeheimnis“ verpflichtet, mit dem die Verfügungsmacht des Medienunternehmens über journalistische Daten gesichert werden soll.

Beispielhaft ist die Regelung im Landespressegesetz Baden-Württemberg. Entsprechende, teilweise weniger ausführliche Regelungen bestehen in allen **Bundesländern**.[24]

> *§ 12 LPResseG BW: Datenverarbeitung zu journalistischen und literarischen Zwecken*
>
> *(1) [1]Soweit Unternehmen der Presse und deren Hilfsunternehmen personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten, ist es den hiermit befassten Personen*

[21] BGH 27.11.2009 – 2 StR 104/09 Rn. 38, AfP 2010, 195.
[22] Schulz/Heilmann in Löffler, Presserecht Kommentar, 7. Aufl. 2023, Mediendatenschutz BT Rn. 66 f.
[23] Art. 95 DSGVO.
[24] Art. 1 BayPrG, § 16a BbgPG, § 5 BremPResseG, § 11a HmbPresseG, § 10 HPresseG, § 18a LPrG M-V, § 19 NPResseG, § 12 LPresseG NRW, § 13 LMG Rh-Pf, § 11 MedienG SL, §§ 1a SächsPrG, § 10a LPresseG LSA, § 10 LPresseG SH, § 11a TPG.

> *untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). [2]Bei der Aufnahme ihrer Tätigkeit sind diese Personen auf das Datengeheimnis zu verpflichten. …*
> *(2) [1]Im Übrigen finden für die Datenverarbeitung zu journalistischen oder literarischen Zwecken durch Unternehmen der Presse und deren Hilfsunternehmen von den Kapiteln II bis VII und IX der Verordnung (EU) 679/2016 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) (ABl. L 119 vom 4. Mai 2016, S. 1, ber. ABl. L 314 vom 22. November 2016, S. 72) nur Artikel 5 Absatz 1 Buchstabe f in Verbindung mit Absatz 2, Artikel 24 und 32 sowie von den Vorschriften des Bundesdatenschutzgesetzes (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097) nur § 83 in ihrer jeweils geltenden Fassung Anwendung. [2]Artikel 82 der Verordnung (EU) 679/2016 gilt mit der Maßgabe, dass nur für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f in Verbindung mit Absatz 2, Artikel 24 und 32, § 83 BDSG mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses nach Absatz 1 gehaftet wird. …*

Die hier geregelte Verpflichtung zum **Datengeheimnis** stammt ursprünglich aus § 5 BDSG 1977 und § 5 BDSG 1990. Danach wird den mit Datenverarbeitung betrauten Personen untersagt, „geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen“ (so § 5 Abs. 1 BDSG 1977). Auf diese bis zum Wirksamwerden der DSGVO 2018 bestehende Norm wurde u.a. in § 57 a.F. RStV für die journalistische Tätigkeit Bezug genommen, was in den aktuell geltenden Presse- und Mediengesetzen ihre Fortschreibung erfuhr, nicht aber im BDSG 2017 ebenso wenig wie in der DSGVO.[25]

Die Regelungen zum Datengeheimnis gehen davon aus, dass Datenschutzverstöße individuell durch Personen erfolgen. Inzwischen ist offensichtlich, dass zentrale Gefahren für den Datenschutz technisch bedingt sein können. Das für das „Datengeheimnis“ durch die Technik bzw. von **externen IT-Dienstleistern** ausgehende Risiko wird im Medienrecht nicht konkret benannt. Die Regelungen zum Datengeheimnis sind aber als spezifische Normierungen des allgemeinen Zweckbindungsgrundsatzes zu verstehen.[26] Angesichts der einheitlichen Funktion und Aufgabe der Akteure betrifft das Datengeheimnis nicht nur die Mitarbeiter, sondern auch die Redaktion und den Arbeitgeber.[27]

1.6 Pressekodex

Der **Pressekodex des Deutschen Presserats** ist eine vorwiegend ethische Verpflichtung für Journalisten und dient der publizistischen Selbstkontrolle. Er verpflichtet nicht nur Journalisten, sondern auch Redaktionen und Herausgeber von journalistischen Werken.[28] Diese können aus dem Pressekodex schutzwürdige Interessen i.S.d. Datenschutzrechts ableiten. Der Presserat ist ein seit 1956 bestehender Zusammenschluss großer deutscher Verleger- und Journalistenverbände. § 23 Abs. 1 S. 6 MStV verleiht

[25] Siehe aber, ohne Journalismusbezug, Art. 32 Abs. 4 DSGVO.
[26] Schulz/Heilmann in Löffler (Fn. 22), Mediendatenschutz BT Rn. 61.
[27] So wohl auch Schulz/Heilmann in Löffler (Fn. 22), Mediendatenschutz BT Rn. 61, und im Ergebnis Binder AfP 2022, 98 f.
[28] Weyhe in Paschke/Berlit/Meyer (Fn. 10), 37 Rn. 16; Held in Paschke/Berlit/Meyer (Fn. 10), 74 Rn. 2; Beater (Fn. 8) Rn. 1836.

dem Pressekodex zudem rechtliche Relevanz bei der Wahrung des Rechtsschutzes bei journalistischen Telemedien.[29]

> Ziff. 5 Pressekodex normiert das „**Berufsgeheimnis**“: *Die Presse wahrt das Berufsgeheimnis, macht vom Zeugnisverweigerungsrecht Gebrauch und gibt Informanten ohne deren ausdrückliche Zustimmung nicht preis. Die vereinbarte Vertraulichkeit ist grundsätzlich zu wahren.*

Eine Präzisierung erfolgt im Pressekodex u.a. mit den Richtlinien 5.1. (**Vertraulichkeit**):

> *Hat der Informant die Verwertung seiner Mitteilung davon abhängig gemacht, dass er als Quelle unerkennbar oder ungefährdet bleibt, so ist diese Bedingung zu respektieren. Vertraulichkeit kann nur dann nicht bindend sein, wenn die Information ein Verbrechen betrifft und die Pflicht zur Anzeige besteht. Vertraulichkeit muss nicht gewahrt werden, wenn bei sorgfältiger Güter- und Interessenabwägung gewichtige staatspolitische Gründe überwiegen, insbesondere wenn die verfassungsmäßige Ordnung berührt oder gefährdet ist.*

In den Sätzen 1,2 und 4 der Richtlinie 5.3 (Datenübermittlung) wird das **Redaktionsgeheimnis** geregelt:

> *Alle von Redaktionen zu journalistisch-redaktionellen Zwecken erhobenen, verarbeiteten oder genutzten personenbezogenen Daten unterliegen dem Redaktionsgeheimnis. Die Übermittlung von Daten zu journalistisch-redaktionellen Zwecken zwischen den Redaktionen ist zulässig. … Eine Datenübermittlung ist mit dem Hinweis zu versehen, dass die übermittelten Daten nur zu journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden dürfen.*

1.7 Medienstaatsverträge

Die presserechtlichen Regeln wurden inzwischen auf die Regelungen zum digitalen Journalismus (Fernsehen, Telemedien) übertragen. Im Anwendungsbereich des **Medienstaatsvertrags** (MStV)[30] bestehen dem Presserecht entsprechende gesetzliche Vertraulichkeitsregeln. Gemäß § 1 Abs. 1 MStV sind diese anwendbar auf private und öffentliche Stellen, welche die Verbreitung und die Zugänglichmachung von Rundfunk und Telemedien in Deutschland veranstalten und anbieten. Für den Rundfunk gelten die §§ 3-16 MStV, für Telemedien die §§ 17-25 MStV.

§ 12 und § 23 MStV regelt die „Datenverarbeitung zu journalistischen Zwecken“ bzw. das „**Medienprivileg**“ weitgehend inhaltsgleich. Den mit der Verarbeitung personenbezogener Daten zu journalistischen Zwecken befassten Personen ist es untersagt, diese Daten „zu anderen Zwecken zu verarbeiten (Datengeheimnis)“ (§§ 12 Abs. 1 S. 1, 23 Abs. 1 S. 1 MStV). Sie sind auf das Datengeheimnis zu verpflichten (§§ 12 Abs. 1 S. 2, 23 Abs. 1 S. 2 MStV). Neben den Kap. I (Art. 1-4. allgemeine Bestimmungen), VIII (Rechtsbehelfe, Haftung, Sanktionen), X (delegierte Rechtsakte, Durchführungsrechtsakte) und XI (Schlussbestimmungen) der DSGVO ist nur Art. 5 Abs. 1 lit. f i.V.m. Art. 5 Abs. 2, 24 und 32 DSGVO anwendbar (§§ 12 Abs. 1 S. 4, 23 Abs. 1 S. 4 MStV).

Das Medienprivileg kann durch **Rechte der von der journalistischen Arbeit Betroffenen** über Gegendarstellungen, Verpflichtungserklärungen und Widerrufe und in begrenztem Maße durch Auskunfts- und Berichtigungsansprüche eingeschränkt sein (§§ 12 Abs. 1 S. 8, Abs. 2 u. 3, 23 Abs. 1 S. 8,

[29] Flechsig in Hahn/Vesting, Beck´scher Kommentar zum Rundfunkrecht, 2. Aufl. 2008, § 10 RStV Rn. 32.

Abs. 2 u. 3 MStV). Damit wird der grundrechtliche Datenschutz nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 8 Abs. 2 S. 2 GRCh mit dem Grundrechtsschutz von Presse und Medien nach Art. 5 GG bzw. Art. 11 Abs. 2 GRCh zum Ausgleich gebracht.[31] Die eigenen Interessen von IT-Dienstleistern für Journalisten haben gegenüber diesen Grundrechten nur eine nachrangige Bedeutung.

1.8 Technisch-organisatorische Garantien

Gemäß sämtlichen medienrechtlichen Regelungen (i.V.m. Art. 85 Abs. 2 DSGVO) sind bei Wahrung der journalistischen Unabhängigkeit keine datenschutzrechtlichen Abstriche hinsichtlich der „**Integrität und Vertraulichkeit**“ zulässig. Dies betrifft insbesondere die technisch-organisatorischen Maßnahmen und die Sicherheit der Verarbeitung einschließlich der hierfür nötigen Dokumentation (Art. 32 DSGVO i.V.m. Art. 5 Abs. 1 lit. f DSGVO). Es gilt auch für journalistische Hilfs- und Beteiligungsunternehmen (§§ 12 Abs. 1 S. 6, 23 Abs. 1 S. 6, 7 MStV; s.o. I.2).[32] Entsprechende Regelungen enthalten § 43 Abs. 1 NDR-Staatsvertrag, § 37 Ans. 1 MDR-Staatsvertrag sowie sinngemäß § 36 Abs. 2 RBB-Staatsvertrag. Die datenschutzrechtlichen Begriffe finden im Medienrecht Anwendung. Dabei geht es nicht nur um die Umsetzung technischer Ziele, sondern generell um „Systemdatenschutz“ und damit auch um die Verfügbarkeit und Unversehrtheit der Daten sowie die Beschränkung des Zugangs und des Zugriffs auf die Daten.[33]

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.[34] Vertraulichkeit von datenbasierten Informationen wird durch die zweckgebundene Abschottung der zugrundeliegenden Daten und die Sicherstellung der Nichtverkettbarkeit erreicht. Es geht somit um eine datenschutzgerechte Systemgestaltung von IT.[35]

Integrität kann sich sowohl auf die Unversehrtheit von Daten als auch auf die korrekte Funktionsweise von Systemen beziehen. Jede unzulässige Veränderung derartiger Schutzobjekte stellt eine Integritätsverletzung dar.[36] Die Erhaltung von Integrität setzt stets voraus, dass der jeweilige Verantwortliche den Umgang mit den Schutzobjekten sicher kontrollieren und bei Bedarf jederzeit intervenieren kann..[37]

Um Integrität und Vertraulichkeit von Daten und den verarbeitenden IT-Systemen nachweisen zu können sind sowohl der Umgang mit den Daten als auch der Betrieb der verarbeitenden IT-Systeme zu dokumentieren. Die **Dokumentationspflicht** obliegt dem Verantwortlichen (Art: 5 Abs. 2 DSGVO). Beim Einsatz von IT-Dienstleistern kann die Rechenschaftspflicht durch die schiere Datenmenge, eine Vielzahl beteiligter Akteure, die Komplexität der Verarbeitung, die Art der Vernetzung und beteiligter Schnittstellen sowie durch Rollenwechsel der Beteiligten gefährdet sein.[38] Sie wird verletzt, wenn – wie etwa bei Microsoft (s.u. 2.1) – dem Verantwortlichen die Dokumentation wesentlicher Gestaltungsaspekte und Verarbeitungsvorgänge vorenthalten wird.

[31] Weichert in Däubler/Wedde/Weichert/Sommer (Fn. 17), Art. 85 Rn. 46.
[32] Hennemann in Specht/Mantz (Fn. 17), S. 546 f. (§ 19 Rn. 55-60).
[33] ErwGr. 39 DSGVO; Roßnagel in Simitis/Hornung/Spiecker (Fn. 18), Art. 5 Rn. 167.
[34] Hansen in Simitis/Hornung/Spiecker (Fn. 18), Art. 32 Rn. 39.
[35] Roßnagel in Simitis/Hornung/Spiecker (Fn. 18), Art. 5 Rn. 169-172.
[36] Hansen in Simitis/Hornung/Spiecker (Fn. 18), Art. 32 Rn. 40.
[37] Rost in Schmidt/Weichert, Datenschutz, 2012, S. 356 f.
[38] Roßnagel in Simitis/Hornung/Spiecker (Fn. 18), Art. 5 Rn. 187.

Sofern die Nutzung von IT-Systemen bei IT-Dienstleistern mit einer wirksamen **Anonymisierung** einhergeht, würde die Betroffenheit i.S.d. Datenschutzrechts entfallen, da es sich bei anonymisierten Daten nicht mehr um personenbezogene Daten im Sinne des Datenschutzrechts handelt. Dies gilt auch für Wahrung der Vertraulichkeit journalistisch verarbeiteter Daten. Allerdings setzt dies die tatsächliche, also unumkehrbare Anonymisierung von Daten voraus. Erfolgt eine Anonymisierung durch einen Auftragsverarbeiter, um danach die „anonymisierten Daten" für eigene Zwecke weiterzuverarbeiten, so ist dies von vielen Voraussetzungen abhängig, u.a. auch davon, dass der Auftragnehmer die Anonymisierungsechnik gegenüber dem Verantwortlichen offenlegen muss.[39]

Zur umfassenden Wahrung der journalistischen Vertraulichkeit bei der Einschaltung von IT-Dienstleistern bedarf es der Anonymisierung von Informanten, der von der Recherche betroffenen Personen sowie der Journalisten selbst. Die Verwendung von Pseudonymen erfüllt diese Voraussetzung nicht, weil die Zuordnung durch Zusatzwissen eine Zuordnung auch für den IT-Dienstleister theoretisch ermöglicht.[40] **Zusatzwissen** ist bei journalistischen Recherchen sogar öffentlich zugänglich, wenn namentliche Veröffentlichungen den Recherchen und Auswertungen zuordenbar sind. Regelmäßig ist zudem aus nicht verschlüsselten Recherche-Inhalten direkt die Identität des Journalisten erkenn- oder zumindest ableitbar.

1.9 Der Journalist im Datenschutzrecht

Ein angestellter Journalist ist aus Datenschutzsicht nicht „Verantwortlicher" i.S.v. Art. 4 Nr. 7 DSGVO; er handelt für den verantwortlichen Arbeitgeber.[41] Der Umstand, dass ein Journalist unter den Gesichtspunkten der Drittwirkung von Grundrechten und staatlicher Schutzpflichten eine **innere Pressefreiheit** gegenüber dem eigenen Arbeitgeber und einen verfassungsrechtlich garantierten Handlungsspielraum genießt, ändert nichts an dieser datenschutzrechtlichen Zuordnung.[42] In Bezug auf die durch ihn verarbeiteten Daten (und resultierende Informationen) ist der Journalist also Teil der verantwortlichen Stelle, seines Arbeitgebers.

In Bezug auf seine eigenen Daten ist der angestellte Journalist gleichzeitig hinsichtlich der Datenverarbeitung durch den Arbeitgeber sowie durch den IT-Dienstleister des Arbeitgebers „betroffene Person" bzw. **Betroffener** (Art. 4 Nr. 1 DSGVO). Als Betroffener hat er die in Art. 12 ff. DSGVO verbrieften materiellen Rechte sowie die prozessualen Rechte gemäß den Art. 77 ff. DSGVO. Die ihn betreffende Datenverarbeitung erfolgt zwar anlässlich einer journalistischen Tätigkeit i.S.v. Art. 85 Abs. 1 DSGVO. Soweit jedoch seine Daten als Beschäftigter des Medienunternehmens durch den Arbeitgeber oder einen IT-Dienstleister verarbeitet werden, ist Art. 85 DSGVO nicht anwendbar. Es erfolgt eine Datenverarbeitung im Beschäftigtenkontext (Art. 88 DSGVO), keine „ausschließlich zu journalistischen Zwecken" (ErwGr. 153 S. 2 DSGVO).[43] Daher müssen sämtliche Vorgaben der DSGVO sowie der nationalen Umsetzungsregelungen von den Verantwortlichen und von den

[39] Stiftung Datenschutz (Hrsg.), Anonymisierung und Pseudonymisierung von Daten, 2023, Praxisleitfaden (1), Kap. 7.3
[40] Weichert in Däubler/Wedde/Weichert/Sommer (Fn. 17), Art. 4 Rn. 75 f.
[41] Weichert in Däubler/Wedde/Weichert/Sommer (Fn. 17), Art. 4 Rn. 89; Hartung in Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, Art. 4 Nr. 7 Rn. 9.
[42] Schemmer in Epping/Hillgruber (Fn. 7), Art. 5 Rn. 50; Kaiser in Dreier, (Fn. 7), Art. 5 I, II Rn. 264 f..; Weber, Innere Pressefreiheit als Verfassungsproblem, 1973.
[43] Dix in Simitis/Hornung/Spiecker (Fn. 18), Art. 85 Rn. 16.

Auftragsverarbeitern beachtet werden.[44] Dies gilt auch für das gemäß der Medienfreiheit privilegierte Medienunternehmen, da der Arbeitgeber in Bezug auf seine Beschäftigten keine journalistischen Zwecke verfolgt.

Der Journalist hat als Betroffener einen grundrechtlich begründeten **Anspruch auf Auskunft** über die ihn betreffenden personenbezogenen Daten (Art. 15 DSGVO, Art. 8 Abs. 2 S. 2 GRCh). Adressat dieses Anspruchs ist der Arbeitgeber als Verantwortlicher.[45] Erfolgt durch den Arbeitgeber eine Inanspruchnahme eines IT-Dienstleisters, der als (gemeinsam) Verantwortlicher zu behandeln ist, so besteht ein direkter Auskunftsanspruch auch diesem gegenüber (Art. 26 Abs. 3 DSGVO).[46] Der IT-Dienstleister und der journalistische Arbeitgeber können in der Vereinbarung nach Art. 26 Abs. 1 DSGVO die Art der die Wahrnehmung der Betroffenenrechte festlegen.[47]

2 IT-Dienstleistung am Beispiel von Microsoft-Produkten

Journalistische Vertraulichkeit kann durch das **Auslesen der Kommunikation und der Datenverarbeitung** des Journalisten verletzt werden. Nutzt der Journalist digitale Werkzeuge, so muss er sich darauf verlassen können, dass ausschließlich Berechtigte Zugriff auf Daten und Inhalte nehmen können. Dies kann durch geeignete Verschlüsselung gewährleistet werden, wenn der Schlüssel beim Journalisten selbst oder bei der Redaktion liegt.[48] Fehlt es an einem solchen Schutz, so eröffnet dies die Möglichkeit der Kenntnisnahme durch Unberechtigte, sei es beim Arbeitgeber, beim IT-Dienstleister oder evtl. weiteren Dritten.

Kommt bei Verlegern, Rundfunkveranstaltern bzw. deren Redaktionen Informationstechnik zum Einsatz, bei der **Klardaten über Inhalte oder Kommunikationspartner und Kommunikationsumstände** an Externe weitergeben werden, dann liegt hierin eine Gefährdung der Vertraulichkeit. Bei diesen „Externen“ kann es sich im datenschutzrechtlichen Sinn um Auftragsverarbeiter (Art. 4 Nr. 8, 28 DSGVO) oder um eigenverantwortliche Datenverarbeiter (Art. 4 Nr. 7 DSGVO) handeln. Während bei einer Auftragsverarbeitung eine strenge vertragliche Bindung des IT-Dienstleisters gegeben ist, die eine zweckwidrige Datennutzung verbietet, fehlt eine solche umfassende Bindung bei einem eigenverantwortlichen IT-Dienstleister.

Im Folgenden wird die Problematik der Einschaltung externer IT-Dienstleister im journalistischen Bereich am praktisch sehr relevanten **Beispiel Microsofts** behandelt. Verwendet ein Verlag oder ein Rundfunkveranstalter IT-Produkte, die mit Microsoft 365 und Teams vergleichbar sind, so besteht ebenso die im Folgenden beschriebene Problematik der Kenntnisnahme journalistischer Geheimnisse.

2.1 Microsoft 365 und integrierte Kollaborationsanwendungen

Presse- und Rundfunkanbieter nutzen zunehmend das IT-Angebot von Microsoft und insbesondere deren Bürosoftware Microsoft (früher Office) 365, sowie je nach Installation weitere hoch integrierte

[44] Weichert in Däubler/Wedde/Weichert/Sommer (Fn. 17), Art. 85 Rn. 22; Buchner/Tinnefeld in Kühling/Buchner (Fn. 41), Art. 85 Rn. 14.
[45] Däubler, Gläserne Belegschaften, 9. Aufl. 2021, Rn. 524 ff.
[46] Dix in Simitis/Hornung/Spiecker (Fn. 18), Art. 26 Rn. 24, 28.
[47] Däubler in Däubler/Wedde/Weichert/Sommer (Fn. 17), Art. 26 Rn. 12; Hartung in Kühling/Buchner (Fn. 41), Art. 26 Rn. 56; Schreibauer in Eßer/Kramer/von Lewinski (Auernhammer), DSGVO BDSG, 8. Aufl. 2024, Art. 26 Rn. 16.
[48] Hansen in Simitis/Hornung/Spiecker (Rn. 14), Art. 32 Rn. 35.

Anwendungen zur Zusammenarbeit. Darunter fallen insbesondere das Kommunikationstool Teams, die Online-Datenablage OneDrive, die Webanwendung SharePoint, das Mailmanagement mittels Exchange und Outlook, aber auch Sicherheitskomponenten wie Defender und weitere. Diese Angebote zeichnen sich dadurch aus, dass Inhalts- und Kommunikationsdaten nicht mehr in der tatsächlichen **Verfügungsmacht** und rechtlichen Verantwortung der Presse- und Rundfunkanbieter verbleiben und dass wesentliche Teile der Datenverarbeitung in die Microsoft-Cloud (Azure) verlagert werden, über die weder die journalistisch Nutzenden noch deren Arbeitgeber eine faktische Kontrolle haben. Die Verlagerung der Datenverarbeitung vom Anwenderrechner bzw. dem Redaktionsrechner zu externen Cloud-Anbietern hat bei vielen journalistischen Einrichtungen schon sehr viel früher begonnen, zumeist mit der Auslagerung von Infrastruktur. Das IT-Angebot von Microsoft verbindet die Dienstleistung einer reinen Infrastructure-as-a-service (IaaS) mit darauf aufbauenden Ebenen wie der Platform-as-a-service (PaaS) und schließlich Software-as-a-service (SaaS). Die mit dieser Auslagerung verbundene Gefährdung der Vertraulichkeit wurde bisher wenig reflektiert, insbesondere, weil die Verarbeitung durch Microsoft nicht ausreichend offengelegt wurde. Mit dem Wechsel zu Office/Microsoft 365, Teams und weiteren Komponenten wird die Verlagerung in die Cloud hinsichtlich aller relevanter Kommunikations- und Inhaltsdaten vorgenommen, so dass Microsoft faktisch von all diesen Daten Kenntnis nehmen kann.

Die deutschen **Datenschutzbehörden** diskutieren schon seit langem mit Microsoft wegen seines aus Datenschutzsicht problematischen Angebots: Selbst nach mehrfacher Überarbeitung der Dokumente zur Clouddatenverarbeitung blieb bis heute offen, welche Daten Microsoft für eigene Zwecke verwendet. Bei jedem Software-Update werden Tausende Änderungen vorgenommen, die weder nachvollziehbar, geschweige denn für die Nutzer ausreichend und verständlich dokumentiert sind. Das Unternehmen teilt nur eingeschränkt mit, welche Unterauftragnehmer beauftragt werden und für welche Zwecke diese Personendaten erhalten. Die Datenschutzbehörden stellten im November 2022 fest, dass Microsoft 365 nicht datenschutzkonform eingesetzt werden kann.[49] Der Versuch einer datenschutzrechtlichen Reinwaschung von Microsoft 365 durch die Anwaltskanzlei Reuschlaw misslang, da zu zwingenden Datenschutzanforderungen der DSGVO keine klaren Feststellungen oder nachvollziehbaren Fakten vorgelegt wurden.[50] Microsoft reagierte auf die Kritik der Datenschutzbehörden mit einem seit Anfang 2023 geltenden „Data Protection Addendum“ (DPA). Angeblich erfolgt die Eigennutzung der Daten erst nach Anonymisierung. Diese wird von Microsoft selbst durchgeführt und weder der Algorithmus noch die verbundenen Abläufe können von Nutzenden und Verantwortlichen überprüft werden. Die Behauptung Microsofts, es würde sich den Weisungen der auftraggebenden Anwender unterwerfen, entbehrt jedes technischen und organisatorischen Belegs.

In Reaktion hierauf veröffentlichte der Landesbeauftragte für den Datenschutz Niedersachsen eine gemeinsam mit sechs weiteren Aufsichtsbehörden erarbeitete „**Handreichung** für die

[49] AG DSK, „Microsoft-Onlinedienste“, Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf; dazu Weichert, CuA 2/2023, 31 ff.

[50] Stellungnahmen zu Microsoft 365: Eine Gegenüberstellung der wesentlichen Aussagen der Datenschutzkonferenz und von Microsoft Eine Übersicht von Stefan Hessel, LL.M. und Christina Kiefer, LL.M. Stand: 28.11.2022; vgl. Hessel/Kiefer, Microsoft 365: Microsoft bewegt sich, die Datenschützer mauern unverhältnismäßig, 09.12.2022, https://heise.de/-7370920.

Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gem. Art. 28 Abs. 3 DSGVO mit Microsoft für den Einsatz von `Microsoft 365´“, in der die Problematik der Nutzung von Microsoft 365 dargestellt wird und in der für eine ansatzweise akzeptable Datenverarbeitung folgende „Hinweise“ gegeben werden[51]: Die Verarbeitung soll auf eigenen IT-Strukturen („On-Premises-Lösung“) erfolgen. Es sollen pseudonymisierte Mail-Adressen und Accounts genutzt werden. Die im „Addendum“ aufgeführten Löschfristen müssen vertraglich angepasst werden; zusätzliche Informationen zu Unterauftragsverarbeitern müssen eingeholt werden. Ungeklärt sei weiterhin der Umgang mit der Verarbeitung durch Microsoft zu eigenen Geschäftszwecken. Eine datenschutzrechtliche Bewertung sämtlicher technischer Funktionen von „Microsoft 365“ sei daher nicht möglich.[52]

Die Nutzung von Microsoft 365 ist also **datenschutzkonform nicht möglich**; es gibt keine Garantie dafür, dass Inhalts- und Kommunikationsdaten von Nutzenden nicht nur Microsoft zur Kenntnis gelangen, sondern dass diese auch von dem Konzern ohne Kontrollmöglichkeit der Nutzenden weitergenutzt werden.

Entsprechendes gilt für das Kollaborations- und Kommunikationswerkzeug Microsoft „**Teams**“, das von Verlegern und Rundfunkanbietern nicht nur als Videokonferenz-Tool, sondern auch für die journalistische Telefonie verwendet wird. Auch dieses Tool, das oft in Kombination mit Microsoft 365 genutzt wird, genügt entgegen den Unternehmensbeteuerungen[53] nicht den datenschutzrechtlichen Anforderungen.[54]

Sämtliche integrierten Komponenten wie OneDrive, SharePoint, Defender u.a. leiden konzeptionsbedingt unter dem gleichen Mangel der Unkontrollierbarkeit durch den verantwortlichen Auftraggeber.

2.2 Daten in den USA

Ein zusätzliches Problem besteht darin, dass Microsoft ein **US-Unternehmen** ist, das dem sicherheitsbehördlichen Zugriff in den USA ausgesetzt ist. Die US-Gesetzgebung, insbesondere über den Foreign Intelligence Surveillance Act (FISA 702) und den Cloud-Act, verpflichtet US-Unternehmen unabhängig von dem Standort der Datenverarbeitung und ohne Rücksicht auf geltende Vertraulichkeits- und Zweckbindungsnormen anderer Staaten, Daten zur Verfügung zu stellen.[55] Die Veröffentlichungen von Edward Snowden haben offengelegt, dass von diesen Befugnissen von US-Behörden, insbesondere von der National Security Agency (NSA), übermäßig Gebrauch gemacht wurde.[56] An dem Bestehen der Zugriffsrechte haben auch die jüngsten normativen

[51] Stand 24.08.2023, https://lfd.niedersachsen.de/download/199434.
[52] LfD Nds, Einsatz von Microsoft 365: Praxis-Tipps für Verträge mit Microsoft, 18.10.2023, https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/einsatz-von-microsoft-365-praxis-tipps-fur-vertrage-mit-microsoft-225722.html.
[53] Sind Microsoft 365 und Microsoft Teams datenschutzkonform? Die Antwort lautet „Ja!“, 17.08.2022, https://news.microsoft.com/de-de/sind-microsoft-365-und-microsoft-teams-datenschutzkonform-die-antwort-lautet-ja/.
[54] Vgl. z.B. Datenschutzerklärung für Microsoft Teams, 28.04.2022, https://www.e-recht24.de/dsg/12701-microsoft-teams.html.
[55] Bergt CR 2023, 629 ff.; Rath/Keller CR 2022, 682 ff.
[56] Greenwald, Die globale Überwachung, 2014, insbes. S. 297 ff.; Snowden, Permanent Record, 2019, S. 278 ff., 316; Rosenbach/Stark, Der NSA Komplex, 2014; Harding, Edward Snowden, 2014; Gellman, Der dunkle Spiegel, 2020.

Eingrenzungsversuche durch die US-Regierung nichts geändert.[57] Es gibt zudem keine Hinweise darauf, dass Datenzugriffe durch US-Behörden nun einer wirksamen rechtsstaatlichen Kontrolle unterliegen.[58] Das Risiko, dass über US-Unternehmen journalistische Erkenntnisse behördlich abgegriffen werden, würde für den Fall erhöht, dass im November 2024 Donald Trump erneut zum US-Präsidenten gewählt würde und so direkten Einfluss auf nationale Ermittlungsbehörden nehmen kann.

Hinsichtlich **journalistischer Daten** ist das Risiko besonders groß. Journalisten recherchieren kritisch auch in den für US-Behörden und insbesondere für die NSA relevanten Bereichen. Es ist davon auszugehen, dass über die Cloud-Datenverarbeitung Microsofts die NSA weiterhin an Daten gelangt. Im Falle einer Nutzung von Cloudangeboten von in den USA beheimateten Unternehmen wie Microsoft würde so das Vertraulichkeitsversprechen deutscher Journalisten verletzt werden. Es ist letztlich eine Frage digitaler Souveränität, dass journalistische Daten in einem Rechtskreis verarbeitet werden, in dem Medienfreiheit und Datenschutz rechtsstaatlich gewährleistet werden.[59]

2.3 Kommunikative Selbstbestimmung?

Die umfassende Überantwortung des Kommunikationsmanagements an Microsoft hat zur Folge, dass Microsoft in der Lage ist, jede Form **unerwünschter Kommunikation** zu unterbinden. Dies erfolgt z.B. durch das Abweisen von Mails über die integrierte Mail-Komponente Outlook in Verbindung mit einem Exchange-Server. Das Abweisen solcher Mails kann den sinnvollen Zweck der Verhinderung von Spam, des Einschleusens von Viren oder sonstiger Schadsoftware haben. Tatsächlich musste bei Microsoft festgestellt werden, dass nicht nur virenverseuchte Mails ausgesondert werden, sondern auch Mail-Kommunikation von besonders vertraulichkeitswahrenden Mailangeboten, so wie dies z.B. bei verschlüsselten Tutanota-Mails der Fall war.[60] Hierin lag ein Verstoß gegen die Vorgaben des Art. 32 i.V.m. Art. 5 Abs. 1 lit. f DSGVO. Das Tutanota-Mailangebot wird von Investigativreportern wegen der integrierten Verschlüsselung verwendet. Es ermöglicht Whistleblowern einen anonymen Austausch mit Journalisten.[61]

Journalisten, Redaktionen und Medienunternehmen müssen Kontrolle über ihre Erreichbarkeit haben. Ohne eine vollständige Kontroll- und ohne eine Einflussmöglichkeit auf die eigene Erreichbarkeit ist es einem Journalisten nicht möglich, die eigene Kommunikation zu steuern. Es ist offenbar nicht gewährleistet, dass Microsoft diese **Steuerungsmöglichkeit** einräumt. Die journalistische Kommunikation kann beobachtet und sabotiert werden. Eine intransparente fremdgesteuerte Kommunikationssteuerung durch Microsoft ermöglicht es dem Unternehmen zudem, Konkurrenten bei der Kommunikation auszuschließen.

---

[57] Zur Problematik des Angemessenheitsbeschlusses der EU-Kommission am 11.07.2023 zum EU-US-Data Privacy-Framework (DPF) Weichert CuA 10/2023, 17 f.; deskriptiv DSK, Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023, 04.09.2023; vgl. DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, 31.01.2023.
[58] Bergt CR 2023, 629 ff.; Rath/Keller CR 2022, 682 ff.
[59] Bizer in Lühr/Jabkowski/Semntek, Handbuch Digitale Verwaltung, 2019, S. 23 ff.
[60] Outlook markiert E-Mails von tutanota.com als Spam, www.golem.de 06.12.2023; Update: E-Mails von Tutanota.com landen nicht mehr im Spamordner von Outlook, https://tuta.com 06.12.2023.
[61] So erreichen Sie das Investigativ-Team der Süddeutschen Zeitung, https://www.sueddeutsche.de/projekte/kontakt/.

3 Medienanbieter und IT-Dienstleister aus Datenschutzsicht

Die Wahrung der journalistischen Vertraulichkeit und Unabhängigkeit ist davon abhängig, ob der Medienanbieter die umfassende Verfügungsmacht über die journalistischen Daten hat. Dabei ist tatsächlich und rechtlich zu unterscheiden zwischen einer weisungsabhängigen Auftragsverarbeitung und einer eigenverantwortlichen Tätigkeit des IT-Dienstleisters. Die Regelungen der DSGVO zur **Verantwortlichkeit** und zur Auftragsverarbeitung sind wegen der Medienprivilegierung des Art. 85 DSGVO nicht direkt anwendbar.[62] Da sie aber Ausdruck einer allgemeinen Rechte- und Pflichtenzuordnung sind, können sie entsprechend angewendet werden.[63]

3.1 Auftragsverarbeitung

Aus datenschutzrechtlicher Sicht besteht ein Unterschied, ob hinsichtlich der Einschaltung eines IT-Dienstleisters eine Auftragsverarbeitung gemäß Art. 28 DSGVO besteht oder nicht. Bei einer Auftragsverarbeitung besteht eine strenge Weisungsabhängigkeit des Auftragsverarbeiters vom verantwortlichen Datenverarbeiter. Durch den Auftragsvertrag gemäß Art. 28 Abs. 3 DSGVO kann der Verantwortliche präzise festlegen, wie die Verarbeitung beim Auftragnehmer zu erfolgen hat. Der Auftragnehmer kann zwar Inhalts- und Kommunikationsdaten zur Kenntnis nehmen, doch ist ihm die Nutzung der Daten **für eigene Zweck untersagt** (vgl. Art. 28 Abs. 10 DSGVO).

Der Auftragsverarbeiter ist zur **Mandantentrennung**, also zur nach Auftraggebern getrennten Verarbeitung der im Auftrag verarbeiteten Daten verpflichtet.[64].

Bei Auftragsverarbeitern von Berufsgeheimnisträgern sind deren Beschäftigte vertraglich zur Vertraulichkeit zu verpflichten (§ 203 Abs. 4 S. 2 Nr. 2 StGB) mit der Folge, dass sich das Berufsgeheimnis auf diese erstreckt und sie als „Mitwirkende“ bei Verstößen strafrechtlich verantwortlich gemacht werden können.[65] Diese Erweiterung der Vertraulichkeitspflicht basiert auf der Erkenntnis, dass geheimhaltungspflichtige Stellen und Personen bei ihrer Datenverarbeitung auf die Inanspruchnahme von IT-Dienstleistern angewiesen sind und daher die Geheimhaltungspflicht auf diese erstreckt werden muss.

3.2 Verantwortlicher IT-Dienstleister

Missachtet ein IT-Dienstleister die rechtlichen Grenzen der Auftragsverarbeitung und bestimmt zumindest teilweise die Zwecke der Datenverarbeitung selbst, so gilt er als Verantwortlicher (Art. 28 Abs. 10 DSGVO). Da auch der Arbeitgeber des Journalisten, der den IT-Dienstleister beauftragt, Verantwortlicher ist, besteht zwischen diesem und dem IT-Dienstleister eine **gemeinsame Verantwortlichkeit** (Art. 26 DSGVO).[66]

---

[62] Binder AfP 2022, 99.
[63] Tendenziell ebenso Datenschutzkonferenz (DSK), 09.11.2017, Umsetzung der DSGVO im Medienrecht; dazu Stender-Vorwachs/Lauber-Rönsberg in Wolff/Brink, Datenschutzrecht, 2. Aufl. 2022, Art. 85 Rn. 45.4.
[64] DSK, Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur - Orientierungshilfe Mandantenfähigkeit, Version 1.0 v. 11.10.2012, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/04/Mandantenf%C3%A4higkeit.pdf; Weichert NZA 2023, 16.
[65] Dazu ausführlich Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, S. 81 ff., https://library.oapen.org/bitstream/handle/20.500.12657/53446/external_content.pdf.
[66] Weichert NZA 2023, 15.

Eine solche gemeinsame Verantwortlichkeit mit der damit verbundenen Offenlegung personenbezogener Daten an den IT-Dienstleister bedarf einer Legitimation gemäß Art. 6 Abs. 1 DSGVO. Bei IT-Dienstleistern für Journalisten kommt als Rechtsgrundlage für diese Übermittlung ausschließlich Art. 6 Abs. 1 lit. f DSGVO in Betracht. Die Datenübermittlung muss „für die **Wahrung der berechtigten Interessen** des Verantwortlichen oder eines Dritten erforderlich (sein), sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“. Die Erforderlichkeit einer „berechtigten“ Eigennutzung der im Auftrag verarbeiteten Daten ist in solchen Fällen regelmäßig fraglich. Dies gilt insbesondere, wenn der IT-Dienstleister – wie Microsoft bei seinem Angebot (s.o. 2.1) – gegenüber den Nutzenden nicht konkret offenlegt, welche Daten für welche Zwecke in Anspruch genommen werden.

In jedem Fall stehen bei einer Datenverarbeitung zu journalistischen Zwecken eines eigenverantwortlichen IT-Dienstleisters **schutzwürdige Betroffeneninteressen** entgegen: Betroffen sind Informanten des Journalisten, der Journalist selbst sowie möglicherweise weitere Personen, die Gegenstand der recherchierten Information des Journalisten sind. Diese Informationen bedürfen eines besonders vertraulichen Umgangs, der bei einer unkontrollierbaren Eigennutzung (wozu insbesondere eine nur behauptete Anonymisierung gehört) durch den IT-Dienstleister nicht gewährleistet ist. Daher ist eine Beauftragung von IT-Dienstleistern im journalistischen Bereich unzulässig, bei der nicht sämtliche Anforderungen des Art. 28 DSGVO zur Auftragsverarbeitung beachtet werden. IT-Dienstleistungen müssen sich auf reine Hilfstätigkeiten beschränken (s.o. 1.2). Dies ist beim Einsatz von Microsoft 365 und seiner integrierten Komponenten nicht der Fall.

4 Individualrechtliche Pflichten des Arbeitgebers

Zwischen angestellt arbeitenden Journalisten und einem Verlag oder Rundfunkveranstalter besteht ein **Arbeitsvertrag**. Derartige Verträge enthalten i.d.R. keine Aussagen zur Auslagerung der beruflich verwendeten IT. Aus den Besonderheiten der Presse- und Rundfunkfreiheit ergeben sich aber besondere arbeitsrechtliche Anforderungen.[67]

4.1 Arbeitsvertrag

Die Arbeitsverträge mit Journalisten verweisen i.d.R. auf deren berufsbedingte Vertraulichkeitspflichten. Dies kann über einen Hinweis auf die geltenden gesetzlichen Regelungen oder auf den Pressekodex erfolgen. Teilweise wird eine ausdrückliche **Vertraulichkeitsverpflichtung** eingefordert, so etwa durch eine öffentlich-rechtliche Rundfunkanstalt:

> *Verpflichtung zur Vertraulichkeit*
> *Ich bin ich persönlich dafür verantwortlich, dass*
> - *mir anvertraute Daten und Datenträger unter Verschluss gehalten werden,*
> - *Daten, Programme und andere Informationen zu keinem anderen als dem konkreten dienstlichen oder vertraglichen Zweck abgerufen oder vervielfältigt werden,*
> - *meine IT-Geräte (z.B. PC, Smartphone, IP-Kamera), meine Anwendungen und meine Passwörter keinem Unbefugten zugänglich gemacht, sowie nicht mehr benötigte personenbezogene Datenträger datenschutzgerecht vernichtet werden, damit eine missbräuchliche Weiterverwendung ausgeschlossen ist,*

[67] Kaiser in Dreier (Fn. 7), Art. 5 I, II Rn. 266.

- *Daten nur entsprechend den mir zugewiesenen Aufgaben verwendet und nicht für private Zwecke gebraucht werden dürfen."*

Mir ist bekannt, dass Verstöße gegen die Vertraulichkeit personenbezogener Daten sowohl zivil- als auch strafrechtlich verfolgt werden können und insbesondere zu Schadenersatzansprüchen oder Bußgelder führen können. Sie können auch Anlass zu rechtlichen Maßnahmen bis hin zur Beendigung des Vertragsverhältnisses sein.

In mehr oder weniger detaillierter Form gelten entsprechende Verpflichtungen für **Journalisten** in jedem Anstellungsverhältnis.

Während also die vertragliche Verpflichtung zur Wahrung der Vertraulichkeit durch den Journalisten sowohl gesetzlich wie auch arbeitsvertraglich abgesichert ist, gibt es keine solchen ausdrücklichen **Verpflichtungen für die Arbeitgeber** gegenüber seinen Journalisten.

Das Fehlen einer expliziten Norm ändert aber nichts an dem Umstand, dass die Arbeitgeber gegenüber ihren angestellten Journalisten und Redakteuren einer Verpflichtung zur Wahrung ihrer beruflichen Vertraulichkeit unterliegen. Diese besteht als **Schutzpflicht des Arbeitgebers** gegenüber den Beschäftigten und ergibt sich in Ermangelung einer spezialgesetzlichen Regelung aus § 241 Abs. 2 BGB, der folgenden Wortlaut hat: *Das Schuldverhältnis kann nach seinem Inhalt jeden Teil zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichten.*

Zudem sind Vertragspartner gemäß § 242 BGB zur **Leistung nach Treu und Glauben** verpflichtet.

Aufgrund der §§ 241 Abs. 2, 242 BGB kann jede Partei nach dem Inhalt des Schuldverhältnisses zur Rücksichtnahme auf die Rechte, Rechtsgüter und Interessen ihres Vertragspartners verpflichtet sein. Arbeitgeber sind gehalten, die im Zusammenhang mit dem Arbeitsverhältnis stehenden **Interessen des Arbeitnehmers** so zu wahren, wie dies unter Berücksichtigung der Interessen und Belange beider Vertragsparteien nach Treu und Glauben verlangt werden kann.[68] Dies wurde früher Fürsorgepflicht genannt und begründet Rücksichts-, Schutz- und Förderpflichten im Arbeitsverhältnis. Die Rücksichtnahmepflicht kann es einer Vertragspartei auch gebieten, die Interessen der anderen Partei aktiv gegenüber Dritten wahrzunehmen.[69]

Die Schutzpflicht besteht auch dahingehend, dass es dem Journalisten ermöglicht wird, seinen journalistischen Geheimhaltungspflichten zu genügen. Zielrichtung dieser Schutzpflicht ist die Möglichkeit zur **Wahrung der beruflichen Obliegenheit** zur Geheimhaltung.

4.2 Gesetzliche Grundlagen

Inwieweit die **mediengesetzlichen Pflichten** (s.o. 1.4-1.6) zur Wahrung der Vertraulichkeit Pflichten des Medienunternehmens Ansprüche von deren Beschäftigten begründen, ist bisher nicht geklärt.

Eine Schutzpflicht des Arbeitgebers besteht explizit hinsichtlich des **Persönlichkeitsschutzes der beschäftigten Journalisten**.[70] Diese ergibt sich allgemein aus § 75 Abs. 2 Betriebsverfassungsgesetz (BetrVG) (allgemeiner § 2 Abs. 1 BPersVG, § 2 Abs. 1 LPersVG BW) und spezifisch für den Datenschutz

[68] BAG 24.10.2018 – 10 AZR 69/19, Rn. 25, NZA 2019, 164.
[69] BGH 14.03.2012 - VIII ZR 220/11, Rn. 23, NJW 2012, 2184.
[70] Schmidt in Erfurter Kommentar zum Arbeitsrecht (Fn. 7), 10 Art. 2 GG Rn. 68.

aus der DSGVO und dem BDSG, insbesondere aus Art. 88 DSGVO und § 26 BDSG.[71] Der Persönlichkeitsschutz von Journalisten hat eine hohe Relevanz: Journalisten sind wegen ihrer Tätigkeit oft besonders gefährdet. Diese werden oft gezielt ausgeforscht, nicht zuletzt auch von staatlichen Geheimdiensten, die sich hieraus Erkenntnisse verschaffen, die sie auf andere Weise nicht erlangen können. Dies gilt auch für US-amerikanische Geheimdienste, die auf US-gesetzlicher Grundlage Zugriff auf von Microsoft als US-Unternehmen verarbeitete Daten nehmen können (s.o. 2.2). Aus einer Ausforschung können sich für einen Journalisten schnell eine Gefährdung für Leib und Leben ergeben.

Zu den Schutzpflichten des Arbeitgebers gehört es, die technischen Voraussetzungen für den **digitalen Schutz der Berufspflichten** und des Persönlichkeitsrechts des Beschäftigten zu schaffen, so wie es seine Aufgabe ist, Schutzkleidung bereitzustellen.[72]

Das Rücksichtnahmegebot kann zudem dazu führen, dass der Arbeitgeber verpflichtet ist, dem Arbeitnehmer diejenigen **Informationen zur Verfügung** zu stellen, die dieser zur eigenen effektiven Interessenwahrnehmung erkennbar benötigt.[73]

4.3 Bring your own device?

Stoßen Journalisten bei ihrem Arbeitgeber auf Widerstand mit ihrer Forderung nach einer vertrauenswürdigen Informationsinfrastruktur, so ist eine naheliegende Reaktion, **eigene als vertrauenswürdige eingeschätzte IT** für die berufliche Tätigkeit zu nutzen. Diese Form der Nutzung wird „Bring your own device“ genannt (BYOD).[74] Dieses pragmatische Vorgehen kann zur Folge haben, dass die datenschutzrechtliche Verantwortung für den Einsatz nicht mehr (nur) beim Arbeitgeber, sondern auch beim Journalisten persönlich liegt. Hat der Arbeitgeber weder Kenntnis noch Kontrolle bzgl. der beruflichen Nutzung eines privaten Dienstes, so ist der Journalist alleine verantwortlich.[75] Besteht Kenntnis von der Nutzung, wird diese vom Arbeitgeber befürwortet und behält er sich insofern ein Weisungsrecht vor, so wird er zum für den BYOD-Einsatz datenschutzrechtlich Verantwortlichen. Dies gilt insbesondere, wenn BYOD in das IT-System des Arbeitgebers, etwa in ein Redaktionssystem, integriert wird. In diesen Fällen ist bei einer vollständigen Beherrschung der Zweckfestlegung von einer Auftragsverarbeitung (Art.28 DSGVO), ansonsten von einer gemeinsamen Verantwortlichkeit von Arbeitgeber und Journalisten (Art. 26 DSGVO) auszugehen.

Eine alleinige oder gemeinsame **Verantwortlichkeit des Journalisten** hat zur Folge, dass ihm (alleine oder gemeinsam) sämtliche Datenschutzpflichten obliegen und ihn ein Haftungsrisiko[76] trifft. Erfolgt die Nutzung des BYOD ohne Wissen des Arbeitgebers, so kann hierin zudem eine Verletzung des Arbeitsvertrags gesehen werden. Konflikte können sich ergeben, wenn der Arbeitgeber eine Herausgabe der während der Arbeitszeit erlangten Ergebnisse einfordert oder bestimmte arbeitsrechtliche Kontrollmaßnahmen vornehmen möchte. Besonders heikel ist es, wenn sich die

[71] Reichold in Münchener Handbuch Arbeitsrecht, Bd. I, Individualarbeitsrecht, 5. Aufl. 2021, § 91 Rn. 9.
[72] BAG, 21.08.1985 - 7 AZR 199/83, NZA 1986, 324; Arbeitsschutzkleidung: In vielen Berufen notwendig, 11.10.2023, https://www.arbeitsrechte.de/arbeitsschutzkleidung/.
[73] Reichold in Münchener Handbuch Arbeitsrecht (Fn. 71); § 91 Rn. 9.
[74] Simon in Arnold/Günther, Arbeitsrecht 4.0, 2ß18, Kap. 1 Rn. 63 f.
[75] Däubler, Digitalisierung und Arbeitsrecht, 8. Aufl. 2022, § 3 Rn. 12; Höller/Wedde in Wedde, Handbuch Datenschutz und Mitbestimmung, 3. Aufl. 2023, H 318 ff.
[76] Günther/Böglmüller in Arnold/Günther (Fn. 74), Kap. 4 Rn. 134-141 (S. 187 f.); Hoppe in Kramer, IT-Arbeitsrecht, 3. Aufl. 2013, § 2 Rn. 752-756 (S. 264 f.).

vermutete Vertraulichkeit des eigengenutzten BYOD als falsch erweist und dadurch Daten kompromittiert werden oder verloren gehen, wofür dann der Journalist verantwortlich ist.

BYOD ist daher keine Lösung für die journalistische Vertraulichkeitspflicht. Sie kann allenfalls übergangsmäßig eine **Notlösung** sein, bei der aber insofern eine schriftliche Absprache zwischen Arbeitgeber und Journalisten nötig ist (Art. 26 oder 28 Abs. 3 DSGVO). Hierbei sollten die relevanten Aspekte (Koppelung mit Redaktions-IT, Kontrolle durch den Arbeitgeber, Verantwortlichkeiten, Haftung, Datenzugriff, Trennung zwischen privater und dienstlicher Nutzung) geklärt werden. Eine Verpflichtung zum Einsatz von BYOD auf Arbeitnehmerseite bzw. zur Akzeptanz einer solchen Nutzung durch den Arbeitgeber besteht für keine der beiden Seiten.[77]

Kommt BYOD nicht nur individuell, sondern generell bei einem Medienunternehmen oder einer Redaktion zum Einsatz, so kann sich hieraus die Notwendigkeit der Einbindung der Beschäftigtenvertretung ergeben, weil **Mitbestimmungssachverhalte** vorliegen (s.u. 5.1 u. 5.3).[78]

5 Kollektivarbeitsrecht

Die vom Arbeitgeber bereitgestellte IT hat nicht nur individualarbeitsrechtliche Bedeutung, sondern betrifft alle Journalisten bzw. Beschäftigten mit kollektivarbeitsrechtlicher Relevanz. Die Beschäftigtenvertretung – der Betriebs- bzw. Personalrat – hat die Aufgabe, die **Rechte der Beschäftigten** gegenüber dem Arbeitgeber zu vertreten. Um dieser Aufgabe nachkommen zu können, hat er Informationsrechte und Mitbestimmungsbefugnisse. Auch berufsspezifische Schutzregeln können von der Beschäftigtenvertretung kollektivrechtlich geltend gemacht werden.

Gemäß § 80 Abs. 1 Nr. 1 BetrVG hat der Betriebsrat „darüber zu wachen, dass die **zugunsten der Arbeitnehmer geltenden Gesetze**, Verordnungen, Tarifverträge, und Betriebsvereinbarungen durchgeführt werden“. § 62 Abs. 2 BPersVG oder z.B. § 68 Abs. 1 Nr. 2 LPersVG BW enthalten für Personalräte entsprechende Regelungen. Zugunsten der Beschäftigten besteht u.a. das Datenschutzrecht.[79] Zwar kennt das kollektive Arbeitsrecht keine spezifischen Regeln für Journalisten. Der Schutzauftrag an die Beschäftigtenvertretung erstreckt sich aber auch auf die medienrechtlichen Regelungen zur Wahrung der Vertraulichkeit.

5.1 Gesetzliche Grundlage

Das **kollektive Arbeitsrecht** unterscheidet zwischen **privaten und öffentlich-rechtlichen Arbeitsverhältnissen**. Arbeitsverhältnisse mit privaten Unternehmen sind einheitlich im BetrVG geregelt. Bei öffentlich-rechtlichen Arbeitsverhältnissen wird danach unterschieden, ob der Arbeitgeber eine Stelle des Bundes ist, was zur Anwendung des BPersVG führt, oder eine Stelle nach Länder, was zur Anwendung von Landesrecht führt.

[77] Däubler (Fn. 75), § 3 Rn. 14 ff. (S. 112 ff.); Hoppe in Kramer (Fn. 76), § 2 Rn. 729 f. (S. 258); Thüsing/Pötters in Thüsing, Beschäftigtendatenschutz und Compliance, 3. Aufl. 2021, § 15 Rn. 30-32 (S. 263).
[78] Däubler (Fn. 75), § 3 Rn. 9 f. (S. 109 f.); Klebe in Däubler/Klebe/Wedde, BetrVG, 18. Aufl. 2022, § 87 Rn. 67 u. 201; Hoppe in Kramer (Fn. 76), § 2 Rn. 732 f., 747-751 (S. 259, 263 f.).
[79] Buschmann in Däubler/Klebe/Wedde (Fn. 78), § 80 Rn. 14.

Öffentlich-rechtliche Anstellungen von Journalisten erfolgen über die Rundfunk- bzw. Medienanstalten. Öffentlich-rechtliche **Medienanstalten des Bundes** sind die Deutsche Welle, das Deutschlandradio und das Zweite Deutsche Fernsehen (ZDF). Auf diese ist das BPersVG anwendbar.

Die **Medienanstalten der Länder** sind der Norddeutsche Rundfunk (NDR, Schleswig-Holstein, Hamburg, Niedersachsen, Mecklenburg-Vorpommern), der Westdeutsche Rundfunk (WDR, Nordrhein-Westfalen), Radio Bremen, der Hessische Rundfunk (HR), Radio Berlin Brandenburg (RBB), der Mitteldeutsche Rundfunk (MDR. Sachsen, Sachsen-Anhalt, Thüringen), der Bayerische Rundfunk (BR), der Saarländische Rundfunk (SR) und der Südwest-Rundfunk (SWR, Baden-Württemberg, Rheinland-Pfalz). Hinsichtlich der Mehrländeranstalten wird in den jeweiligen Staatsverträgen bestimmt, welches Recht anzuwenden ist. Gemäß § 41 Abs. 1 NDR-Staatsvertrag, § 34 Abs. 1 RBB-Staatsvertrag und § 35 Abs. 1 MDR-Staatsvertrag gilt für die Angestellten von NDR, RBB und MDR das BPersVG. Gemäß § 38 Abs. 1 SWR-Staatsvertrag findet das Personalvertretungsgesetz des Landes Anwendung, in dem der Dienstort der Intendanz liegt (Stuttgart § 1 Abs. 1 S. 2 SWR-Staatsvertrag), weshalb das Landespersonalvertretungsgesetz Baden-Württemberg gilt. Bei Einländeranstalten gilt das jeweilige Landespersonalvertretungsgesetz.

5.2 Informationsrechte

Der Arbeitsgeber hat gegenüber dem Betriebsrat gemäß § 80 Abs. 2 BetrVG eine umfassende Unterrichtungsbefugnis zur Verwirklichung der Betriebsratsaufgabe, die Einhaltung der für die Beschäftigten geltenden Schutzregelungen zu überwachen. Ihm sind nach Satz 2 auf Verlangen jederzeit die erforderlichen **Unterlagen** zur Verfügung zu stellen. Die Unterrichtung kann auch durch Beschäftigte als Auskunftspersonen erfolgen (Satz 4) sowie über die Hinzuziehung von externen Sachverständigen (§ 80 Abs. 3 BetrVG).

Diesen Informationsansprüchen können vom Arbeitgeber keine Betriebs- und Geschäftsgeheimnisse entgegenhalten werden (vgl. § 79 Abs. 1 S. 1 BetrVG).[80] Einzige Grenze ist die **Erforderlichkeit für die Wahrnehmung der gesetzlichen Aufgaben** des Betriebsrats. Dazu gehört auch die Möglichkeit zur Feststellung, ob ein mitbestimmungspflichtiger Sachverhalt gegeben ist und die Vorbereitung der Gestaltung mitbestimmungspflichtiger IT-Systeme in Verhandlungen mit dem Arbeitgeber (s.u. 5.3).

Gemäß der Rspr. des BAG ist der Arbeitgeber nach § 80 Abs. 2 BetrVG nicht verpflichtet, nicht vorhandene Unterlagen zu erstellen.[81] Der Betriebsrat hat aber einen Anspruch darauf, dass der Arbeitgeber sich darum bemüht, bei **Vertragspartnern** vorhandene, für die Aufgabenerledigung nötige Unterlagen zu beschaffen. Für die Betriebsratstätigkeit erforderliche Unterlagen sind auch solche, die der Arbeitgeber für seine eigene gesetzliche Aufgabenerfüllung benötigt. Selbst wenn z.B. mit einem Auftragsverarbeiter oder einem gemeinsam Verantwortlichen keine vertragliche Absprache über die Bereitstellung von Unterlagen durch den IT-Dienstleister besteht, so ergibt sich aus der gesetzlichen Informationspflicht des Arbeitgebers gegenüber dem Betriebsrat eine gesetzliche Pflicht des IT-

[80] Weber in GK-BetrVG Bd. II, 11. Aufl. 2018, § 80 Rn. 93; Fitting, Betriebsverfassungsgesetz, 31. Aufl.2022, § 79 Rn. 1; § 80 Rn. 60; Buschmann in Däubler/Klebe/Wedde (Fn. 78), § 80 Rn. 151.
[81] BAG 07.05.2019 – 1 ABR 53/17, Rn. 16, NZA 2019, 1218; zu Recht kritisch Buschmann in Däubler/Klebe/Wedde (Fn. 78), § 80 Rn. 113.

Dienstleisters gegenüber dem Arbeitgeber zur Beschaffung und Bereitstellung dieser Unterlagen (vgl. Art. 28 Abs. 3 lit. a, f u. h DSGVO).[82]

Entsprechendes regelt § 66 Abs. 1 BPersVG: „Der Personalrat ist zur Durchführung seiner Aufgaben rechtzeitig und **umfassend zu unterrichten**. Ihm sind die hierfür erforderlichen Unterlagen, einschließlich der für die Durchführung seiner Aufgaben erforderlichen personenbezogenen Daten, vorzulegen." Gemäß § 68 Abs. 2 S. 1 u. 2 LPersVG BW ist die Personalvertretung „zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten. Ihr sind die hierfür erforderlichen Unterlagen vorzulegen".

5.3 Mitbestimmungstatbestand „Überwachung"

Der Betriebsrat hat ein Mitbestimmungsrecht gemäß § 87 Abs. 1 Nr. 6 BetrVG bei „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen". Es genügt, dass diese Einrichtungen **zur Verhalts- und Leistungskontrolle geeignet** sind. Eine Nutzungsabsicht ist nicht nötig.[83]

IT-Verfahren für die **digitale Arbeits- und Büro-Organisation und -Kommunikation** erfüllen diese Anforderungen.[84] Diesen IT-Verfahren darf im Rahmen der Mitbestimmung durch den Betriebsrat nur zugestimmt werden, wenn sie so gestaltet werden können (und gestaltet werden), dass sie den gesetzlichen Anforderungen genügen. Dies ergibt sich unter anderem aus der Bestimmung aus § 80 Abs. 1 Nr. 1 BetrVG (s.o. 5). Diese Voraussetzung kannbei der üblichen Nutzung von Microsoft 365 und seinen integrierten Komponenten nicht erfüllt werden.

§ 80 Abs. 1 Nr. 21 **BPersVG** oder z.B. § 79 Abs. 3 Nr. 12 LPersVG entsprechen § 87 Abs. 1 Nr. 6 BetrVG. Darüberhinausgehend erstreckt § 79 Abs. 3 Nr. 14 LPersVG Baden-Württemberg die Mitbestimmung auch auf die „Einführung, Anwendung oder wesentliche Änderung oder wesentliche Erweiterung technischer Einrichtungen und Verfahren der automatisierten Verarbeitung personenbezogener Daten der Beschäftigten".

5.4 Wahrung eines menschengerechten Arbeitsumfelds

Gemäß § 91 BetrVG besteht ein Mitbestimmungsrecht bei „**Änderungen der Arbeitsplätze**, des Arbeitsablaufs oder der Arbeitsumgebung, die den gesicherten arbeitswissenschaftlichen Erkenntnissen über die menschengerechte Gestaltung der Arbeit offensichtlich widersprechen" und dadurch die Arbeitnehmer in besonderer Weise belasten. Der Betriebsrat kann in solchen Fällen „angemessene Maßnahmen zur Abwendung, Milderung oder zum Ausgleich der Belastung verlangen". Vom Arbeitgeber neu bereitgestellte IT, mit der Journalisten nicht ihrer Verpflichtung zur Vertraulichkeit genügen können und die sie bei der Entgegennahme von notwendigen Mitteilungen beeinträchtigen, kommen als Anwendungsfälle des § 91 BetrVG in Betracht.[85]

[82] Petri in Simitis/Hornung/Spiecker (Fn. 18), Art. 28 Rn. 64, 81.
[83] BAG 10.12.2013 - 1 ABR 43/12 - Rn. 20 m.w.N., NZA 2014, 439; BAG 27.01.2004 - 1 ABR 7/03 - Rn. 25, NZA 2004, 556; BAG 11.03.1986 – 1 ABR 12/84; BAG 06.12.1983 – 1 ABR 43/81, NJW 1984, 285.
[84] Klebe in Däubler/Klebe/Wedde (Fn. 78), § 87 Rn. 199, 202 m.w.N.; Wiese/Gutzeit in GK-BetrVG 12. Aufl. 2021, § 87 Rn. 576, 583; Outlook-Gruppenkalender LAG Nürnberg 21.01.2017 – 7 Sa 441/16, NZA-RR 303.
[85] Fitting (Fn. 80), § 91 Rn. 10.

Für die „**Änderung**“ gilt keine enge zeitliche Begrenzung: Erst wenn erkannt wird, dass mit der praktischen Änderung sich eine wesentliche Veränderung z.B. bei den Rahmenbedingungen der Arbeit ergibt, kann das Mitbestimmungsrecht wahrgenommen werden.[86]

Die Änderung muss der **menschengerechten Arbeitsgestaltung** widersprechen, um die Mitbestimmungspflicht auszulösen. Anwendungsfälle der Regelung bezogen sich bisher insbesondere auf Gesundheitsrisiken am Arbeitsplatz; sie beschränkt sich jedoch nicht hierauf. Zur Menschengerechtigkeit gehören auch die Wahrung des allgemeinen Persönlichkeitsrechts und der sozialen Angemessenheit.[87] Fundamentale und im System angelegte Verstöße gegen den Datenschutz sowie Einschränkungen der Vertraulichkeit der Kommunikation für Journalisten sind solche nicht menschengerechte Arbeitsumstände.

Die fehlende Menschengerechtigkeit muss **arbeitswissenschaftlich gesichert** sein. Diesen Anforderungen genügen im Hinblick auf den Einsatz von Microsoft 365 und seiner Komponenten die Feststellungen der deutschen Datenschutzaufsichtsbehörden.

Die **besondere Belastung** muss objektiv vorliegen.[88] Sie ist bei Journalisten gegeben, wenn sie sich nicht auf die Vertraulichkeit ihrer Kommunikation und ihrer Arbeitsmittel verlassen können.

Gemäß § 80 Abs. 1 Nr. 4 und Nr. 20 **BPersVG** sind die „Gestaltung der Arbeitsplätze“ die „Einführung grundlegend neuer Arbeitsmethoden“ mitbestimmungspflichtig (ebenso § 79 Abs. 3 Nr. 13 u. Abs. 1 Nr. 10 LPersVG BW).

6 Ergebnis

Es besteht für Journalisten gegenüber ihrem Arbeitgeber ein verfassungsrechtlich, mediengesetzgesetzlich und arbeitsrechtlich begründeter Anspruch darauf, dass bei der Bereitstellung von digitalen Instrumenten zur Informationsbeschaffung, Kommunikation, Auswertung und generell zur Datenverarbeitung die journalistische Arbeit gefördert und nicht gefährdet wird. Sowohl individualrechtlich wie kollektivrechtlich kann der Arbeitgeber hierzu veranlasst werden. Informationstechnik, bei der die Datenverarbeitung intransparent ist und über die Arbeitgeber und Journalisten nur eingeschränkt **Verfügungsmacht** haben, gefährden die **journalistische Vertraulichkeit**.

Diese im Medienbereich bestehende Problematik ist übertragbar auf weitere Beschäftigte, für die besonderen Geheimhaltungsbefugnissen und -pflichten bestehen. Dies ist der Fall bei Ärzten, Psychologen und sonstigen der **beruflichen Schweigepflicht** nach § 203 StGB unterliegenden Personen.[89] Es gilt auch für die Amtsverschwiegenheit gemäß § 203 Abs. 2 StGB.[90]

Beim **Einsatz von Microsoft 365** und den darin eingebundenen Werkzeugen (Tools) insbesondere bei der Nutzung des Kommunikationstools Teams ist eine Gefährdung von Vertraulichkeit und Integrität

[86] Wankel in Däubler/Klebe/Wedde (Fn. 78), § 91 Rn. 5f.
[87] Wankel in Däubler/Klebe/Wedde (Fn. 78), § 91 Rn. 9.
[88] Weber in GK-BetrVG (Fn. 80), § 91 Rn. 17.
[89] BAG 13.01.1987 – 1 AZR 267/85, DB 1987, 1153; Däubler (Fn 75), S. 264 (§ 8 Rn. 67-69); Ernst NZA 2002, 590; Beckschulze/Henkel DB 2001, 1495.
[90] So finden z.B. in der Landesverwaltung Schleswig-Holstein Microsoft 365 und Teams keine Anwendung.

gegeben. Daher ist der journalistische Einsatz dieser IT zu vermeiden. Hierzu können die Arbeitgeber von den bei ihnen angestellten Journalisten rechtlich verpflichtet werden.

Abkürzungen

Abs.	Absatz
AfP	Archiv für Presserecht
AG	Arbeitsgruppe
Art.	Artikel
Aufl.	Auflage
AUV	Vertrag über die Arbeitsweise der EU
B	Bundes-
BAG	Bundesarbeitsgericht
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BVerfG	Bundesverfassungsgericht
BGH	Bundesgerichtshof
BR	Bayrischer Rundfunk
BW	Baden-Württemberg
CR	Computer und Recht (Zeitschrift)
CuA	Computer und Arbeit (Zeitschrift)
DANA	DatenschutzNachrichten
DB	Der Betrieb (Zeitschrift)
DSGVO	Europäische Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
ErwGr	Erwägungsgrund
EU	Europäische Union
EuGH	Europäischer Gerichtshof
f/f.	fort/folgende
Fn.	Fußnote
GG	Grundgesetz
GK-	Gemeinschaftskommentar
GRCh	Europäische Grundrechte-Charta
HR	Hessischer Rundfunk
i.d.R.	in der Regel
IP	Internet Protocol
i.S.d./v.	im Sinne des/von
IT-	Informationstechnik-
i.V.m.	in Verbindung mit
Kap.	Kapitel
L	Landes-
LfD	Landesbeauftragter für Datenschutz
lit.	Buchstabe
MDR	Mitteldeutscher Rundfunk
MMR	Multimedia und Recht (Zeitschrift)
MStV	Medienstaatsvertrag
m.w.N.	mit weiteren Nachweisen
NDR	Norddeutscher Rundfunk
Nds.	Niedersachsen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSA	National Security Agency
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
PC	Personal Computer
PE	Presseerklärung
PersVG	Personalvertretungsgesetz
PresseG	Pressegesetz
RBB	Radio Berlin Brandenburg
Rn.	Randnummer
RSpr.	Rechtsprechung
RStV	Rundfunkstaatsvertrag
S.	Satz/Seite
s.o.	siehe oben
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
s.u.	siehe unten
SWR	Südwestrundfunk
TK-	Telekommunikations-
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
u.	und
u.a.	und andere
US/A	United States/of America

z.B.	zum Beispiel	ZPO	Zivilprozessordnung
ZDF	Zweites Deutsches Fernsehen		