Deutscher Fachjournalisten Verband

Leitfaden "EU-Datenschutz-Grundverordnung (DSGVO) und Journalismus"

von Ass. jur. Anne-Christine Herr und Rechtsanwalt Christian Solmecke

Ab dem 25. Mai 2018 gilt auch in Deutschland die EU-Datenschutz-Grundverordnung (DSGVO). Diese wird zukünftig das Datenschutzrecht europaweit direkt regeln. Lediglich in Details hat der deutsche Gesetzgeber dann noch Handlungsspielraum.

Ein wichtiger Aspekt, den die EU-Staaten selbst regeln müssen, ist das Verhältnis der Presse- und Rundfunkfreiheit zum Datenschutzrecht. Mit dem 25. Mai 2018 gelten zwar die zahlreichen bisherigen Ausnahmen nicht mehr, die das deutsche Recht bislang für Journalisten vorsieht (Presse- bzw. Medienprivileg). Die Länder sind aber dazu berufen, unter anderem in den Landespressegesetzen und dem Rundfunkstaatsvertrag (RStV) neue Regelungen zu schaffen, die weiterhin entsprechende Ausnahmen von der DSGVO für Journalisten vorsehen.

Doch langsam wird die Zeit eng: Nicht alle Länder haben bereits neue Gesetze verabschiedet – und wenn nicht alle Länder rechtzeitig handeln, herrscht teilweise noch Rechtsunsicherheit. Eine Woche vor Inkrafttreten der DSGVO gab es neue Pressegesetze lediglich in Nordrhein-Westfalen (NRW), Mecklenburg-Vorpommern und Schleswig-Holstein. Diese Länder haben auch schon dem neuen RStV zugestimmt.

Immerhin bieten diese Gesetze sowie der RStV-Entwurf bereits gute Einblicke in die Regelungen des Medienprivilegs ab Ende Mai. Journalisten können damit wohl aufatmen: Es bleibt vieles wie bisher.

1. Wozu dient das Medienprivileg?

Das Medienprivileg bezieht sich auf das prinzipielle Spannungsverhältnis zwischen dem Datenschutz und den Grundrechten der Presse.

Der Datenschutz sichert das Grundrecht auf „informationelle Selbstbestimmung“ als Teil des Allgemeinen Persönlichkeitsrechts, welches die Gerichte aus der grundgesetzlich garantierten Handlungsfreiheit und der Menschenwürde abgeleitet haben. Danach sind Menschen grundsätzlich davor geschützt, dass ihre sogenannten „personenbezogenen Daten“ von Dritten verarbeitet werden. Personenbezogene Daten sind alle Informationen, die irgendwie Rückschlüsse auf eine Person zulassen. Entscheidend ist dabei, dass man die Daten mit vertretbarem Aufwand einer bestimmten Person zuzuordnen kann. Beispiele sind: Name, Telefonnummer, E-Mail-Adresse, Kfz-Kennzeichen, IP-Adresse, IBAN. Diejenigen, die solche Daten verarbeiten (Verantwortliche), dürfen dies nur tun, wenn Betroffene eingewilligt haben oder das Gesetz es erlaubt – so stand es schon im Bundesdatenschutzgesetz in der alten Fassung (BDSG a. F.) und so regelt es auch zukünftig die DSGVO. Hinzu kommt, dass diejenigen, deren personenbezogene Daten verarbeitet werden (Betroffene), ein Recht darauf haben, zu erfahren, welche Daten von ihnen verarbeitet werden – sie müssen hierüber informiert werden und haben auch selbst ein Auskunftsrecht gegen Verantwortliche. Schließlich können sie unter gewissen Umständen sogar verlangen, dass gespeicherte Daten über sie gelöscht werden.

Diese Rechte und Pflichten sind jedoch mit der journalistischen Arbeit meist nicht vereinbar. Denn Journalisten haben unter anderem die Aufgabe, investigativ zu recherchieren und Menschen auch über Missstände zu informieren – ohne dass diejenigen, über die berichtet wird, zuvor davon erfahren und diese Arbeit sabotieren könnten. Würden die Datenschutzrechte uneingeschränkt

gelten, dürften Journalisten generell nur über Personen berichten, wenn diese eingewilligt haben oder das Gesetz es sonst erlaubt – zum Beispiel, weil sie sich auf ein „berechtigtes Interesse“ im jeweiligen Einzelfall stützen können. Diejenigen, über die ein Journalist recherchiert, könnten die Presse sogar zur Löschung dieser Daten zwingen – und auch leicht an interne Informationen herankommen. Ein Informantenschutz wäre nicht mehr möglich. Die Presse muss aber unabhängig arbeiten und ihre Quellen schützen können. Und sie braucht – in Grenzen – auch das Recht, Fotos von Personen zu veröffentlichen, über die sie berichtet. Diese Rechte werden durch die Kommunikationsgrundrechte aus Artikel 5 des Grundgesetzes (GG), insbesondere die Presse- und Rundfunk sowie die Meinungsfreiheit, abgesichert.

2. Das Medienprivileg nach der bisherigen Rechtslage

Dieses Spannungsverhältnis wurde nach bislang geltender Rechtslage aufgelöst durch die Öffnungsklausel § 41 Abs. 1 BDSG a. F., umgesetzt durch § 57 RStV für Fernsehen, Rundfunk und Telemedien (Online-Medien) sowie entsprechende Regelungen für Print in den einzelnen Landespressegesetzen: Nach dem Medien- bzw. Presseprivileg gelten die meisten Vorschriften des BDSG a. F. nicht für die journalistisch-redaktionelle Verwendung personenbezogener Daten. Die Regelungen des Medienprivilegs sind bislang weitestgehend gleich, egal ob es sich um Rundfunk-, Print-, eigenständige oder zu Presse bzw. Rundfunk gehörende Online-Angebote handelt.

Nach dem Medienprivileg müssen Medienunternehmen und Journalisten im Rahmen ihrer Tätigkeit fast kein Datenschutzrecht beachten. Einhalten müssen sie aber Vorschriften zum Datengeheimnis und zur Datensicherheit.

Es bedeutet im Einzelnen:

- Im journalistisch-redaktionellen Bereich dürfen sie personenbezogene Daten verarbeiten, ohne hierfür eine gesetzliche Erlaubnis bzw. Einwilligung des Betroffenen zu haben.
- Sie unterliegen keiner staatlichen Datenschutzaufsicht, sondern nur gegebenenfalls der Selbstverpflichtung des Pressekodex des Deutschen Presserats.
- Diejenigen, deren Daten sie verarbeiten, erhalten keine Informationen hierüber, auch haben sie in der Regel keinen datenschutzrechtlichen Anspruch auf Auskunft gegen sie (Ausnahme: § 41 Abs. 3 BDSG a. F., hier bestand ein spezieller Auskunftsanspruch gegen die Deutsche Welle).

Redaktionen müssen derzeit nur folgende Regelungen des BDSG beachten:

- § 5 BDSG – Datengeheimnis;
- § 9 BDSG – die Einhaltung technisch-organisatorischer Maßnahmen (Datensicherheit);
- § 38 a BDSG – Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen durch Berufsverbände;
- § 7 BDSG – Schadensersatz; mit der Maßgabe, dass Journalisten nur für die Verletzung der §§ 5 und 9 BDSG haften.

Doch auch gegenüber der Presse sind Personen natürlich nicht schutzlos. Private Journalisten bzw. Redaktionen, die sich freiwillig dem Pressekodex unterworfen haben – dieser schützt unter

anderem auch das Persönlichkeitsrecht Betroffener –, müssen diesen einhalten. Der Deutsche Presserat übernimmt hier als Organ die Aufgabe der freiwilligen Selbstkontrolle – anstelle staatlicher Behörden. Außerdem können Betroffene sich gegenüber den journalistischen Vertretern immer noch auf ihr allgemeines Persönlichkeitsrecht oder ihr Recht am eigenen Bild berufen und wegen einer Verletzung dieser Rechte Schadensersatz verlangen. Im Rahmen eines solchen Anspruchs prüfen die Gerichte dann, ob die Pressevertreter hier die Grundrechte angemessen beachtet haben.

Die bisherige Rechtslage zum Datenschutz und dem Medienprivileg können Sie in dieser ausführlichen Broschüre des Deutschen Presserats nachlesen.

3. Neue Regelungen bisher nur in drei Ländern

Der Bund hat im BDSG neuer Fassung (n. F.) keine entsprechenden Ausnahmen des Datenschutzrechts für Journalisten vorgesehen – § 41 BDSG a. F. wurde im neuen BDSG gestrichen. Die Anpassungen des Medienrechts liegen jetzt allein in der Kompetenz der Bundesländer. Das Medienrecht ist in Deutschland aber sehr differenziert geregelt – so müssen der RStV, 16 Landespressegesetze (LPG) und Einzelvorschriften für ARD und ZDF angepasst werden.

Derzeit (Stand 18.05.2018) haben lediglich drei Bundesländer (siehe oben) schon entsprechende Gesetze für die Presse erlassen. Die darin enthaltenen Regelungen werden im Folgenden exemplarisch vorgestellt– letztlich unterscheiden sie sich nur in Details. Eine nicht ganz aktuelle Aufstellung der weiteren, derzeit noch in der Diskussion befindlichen Gesetzentwürfe finden Sie hier.

4. Was gilt ab dem 25. Mai für Pressevertreter in Bundesländern ohne Regelung?

Derzeit besteht folgende Situation: § 41 BDSG gibt es ab dem 25. Mai nicht mehr. Der RStV und die Landespressegesetze sehen explizit nur konkrete Ausnahmen des BDSG a. F. vor, nehmen aber keinen Bezug auf die DSGVO. Somit gehen sie ab dem 25. Mai ins Leere. Ergeht vor dem 25. Mai keine Sonderregelung, so müssen Journalisten, die nicht unter die drei (und weitere in den nächsten Tagen) bereits verabschiedeten Pressegesetze fallen, wahrscheinlich die Regelungen der DSGVO einhalten.

Die durch die Rechtsprechung entwickelten Grundsätze zu den bislang geltenden Regelungen können aber zumindest hilfsweise herangezogen werden. Fände die DSGVO tatsächlich Anwendung, könnte man folgendermaßen argumentieren und die wirklich brisanten Normen der DSGVO im Sinne der Pressefreiheit auslegen:

- Im Hinblick auf die Erlaubnis, überhaupt personenbezogene Daten zu verarbeiten, gibt es in der DSGVO eine entsprechende Norm in Art. 6 Abs. 1 lit. f), nämlich wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Diese Norm verlangt letztlich eine Interessen- bzw.

Grundrechtsabwägung. Die Mediengrundrechte dürften im Zweifel überwiegen, um auf dieser Basis über Personen zu recherchieren und in ihr Persönlichkeitsrecht einzugreifen.

- Den Informationspflichten aus Art. 14 DSGVO dürften Journalisten nicht unterliegen, weil die Erteilung dieser Informationen „unmöglich“ ist – schließlich würde sie die Pressearbeit unterminieren.
- Auch der befürchtete Auskunftsanspruch der Personen, über die recherchiert wird, ließe sich wohl mit dem Argument der Grundrechte umgehen. Zwar sieht der Auskunftsanspruch keine direkten Ausnahmen vor, wie es auf Basis der alten Rechtslage der Fall war. Doch die Auskunft darf nach überwiegender Ansicht entsprechend Abs. 4 des Artikel 14 DSGVO verweigert werden, wenn die Rechte und Freiheiten anderer Personen beeinträchtigt würden – dies wäre laut dem dazu gehörigen Erwägungsgrund zum Beispiel bei Persönlichkeitsrechts¬verletzungen Dritter oder bei entgegenstehenden Geschäftsgeheimnissen der Fall. Journalisten können sich hier also auf ihre grundrechtlich geschützte Arbeit und ihr Redaktionsgeheimnis stützen und entsprechende Auskünfte verweigern.

Eine andere, juristisch aber sehr fragliche Möglichkeit ist, sich bis zur Geltung der neuen Regeln vorläufig direkt auf die Öffnungsklausel in Art. 85 DSGVO zu berufen und sich zu verhalten wie bisher unter der alten Rechtslage. Denn die Staaten haben ja einen expliziten Auftrag, Ausnahmen von der DSGVO zu journalistischen Zwecken vorzusehen. Juristisch korrekt ist das Vorgehen aber nicht –und wegen fehlender Rechtssicherheit nicht empfehlenswert.

5. Wer ist überhaupt vom Medienprivileg erfasst?

Erfreulich ist, dass die bisher bekannt gewordenen verabschiedeten Landespressegesetze und der Entwurf zum RStV den **Journalismus-Begriff klarstellen und nur noch von journalistischen Zwecken die Rede ist**. In den bisherigen Regelungen des Medienprivilegs war eine Verarbeitung „ausschließlich zu eigenen journalistisch-redaktionellen“ Zwecken vorausgesetzt – die Einschränkungen „ausschließlich zu eigenen“ und „redaktionellen“ dürften wohl meist nicht übernommen werden; so sehen es auch einige weitere aktuelle Entwürfe, etwa in Hessen. Anlässlich der DSGVO, wonach der Journalismus-Begriff weit zu verstehen ist, wurde wohl einheitlich eine Datenverarbeitung zu journalistischen Zwecken insgesamt privilegiert. Allerdings sind auch weiterhin Entwürfe im Gespräch, die noch die alte Begrifflichkeit verwenden. Letztlich wird das aber für Fachjournalisten keinen großen Unterschied machen, da diese Pressevertreter beide Begriffe erfüllen werden.

Dennoch: Für all diejenigen, die nicht klassisch in eine Redaktion eingebunden sind oder zumindest auch als Blogger, Fotografen oder im PR-Bereich tätig sind, folgt an dieser Stelle ein kurzer Überblick über den voraussichtlichen Anwendungsbereich der neuen Medienprivilegien.

Wer gilt als Journalist?

Zu der Frage, wer eigentlich privilegiert ist, heißt es in der Begründung zum neuen RStV, dass der alte Pressebegriff des BDSG a. F. weiter gelten soll. Diesen hat unter anderem das Bundesverwaltungsgericht (BVerwG) bereits 2015 definiert (Urteil vom 29.10.2015, AZ. 1 B 32/15) und Folgendes klargestellt:

- Das Medienprivileg gilt für die Presse im verfassungsrechtlichen Sinn und damit auch für die Online-Medien, wenn sie unter den Pressebegriff des Art. 5 Abs. 1 Satz 2 GG fallen.
- Der Begriff der Presse ist weit auszulegen. Auch, wenn der RStV und das BDSG a. F. nur von „Unternehmen“ bzw. „Hilfsunternehmen“ bzw. zum Teil von „Beteiligungsunternehmen“ der Presse sprechen, so muss das Medienprivileg auch für selbstständige Journalisten gelten, die nicht in redaktionelle Strukturen eingebunden sind.
- Auch für Kunden-, Werks-, Partei- und Vereinspublikationen wird grundsätzlich anerkannt, dass das Medienprivileg Anwendung findet.
- Vereine, Parteien oder sonstige Unternehmen, die Mitglieder-, Kunden- oder sonstige Publikationen erstellen, können das Medienprivileg nur in Anspruch nehmen, wenn die für die Publikationen zuständige Abteilung organisatorisch selbstständig, in sich geschlossen gegenüber den sonstigen (betrieblichen) Stellen, abgeschottet und in der redaktionellen Tätigkeit als Organisationseinheit autonom ist.
- Ein weites Begriffsverständnis der „Presse“ und der ihr zuarbeitenden Personen bzw. Unternehmen verlangt auch zukünftig die DSGVO. In Erwägungsgrund 153 der DSGVO heißt es:

  „Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.“

So sah es zuvor schon der Gerichtshof der Europäischen Union (EuGH), der zukünftig die Auslegung der entsprechenden Normen bestimmen wird. Nach dem EuGH liegen journalistische Zwecke in jeder Tätigkeit, die es zum Ziel hat, Informationen, Meinungen oder Ideen, mit welchem Übertragungsmittel auch immer, in der Öffentlichkeit zu verbreiten (EuGH 16.12.2008 – C-73/07, EuZW 2009, 108 (110) Tz. 58 – Satamedia). Ähnlich sagte dies der Bundesgerichtshof (BGH) 2011 (Urteil vom 01.02.2011, Az. VI ZR 345/09):

> *„Daten werden dann zu journalistisch-redaktionellen Zwecken verarbeitet, wenn die Zielrichtung in einer Veröffentlichung für einen unbestimmten Personenkreis besteht (…). Es muss die Absicht einer Berichterstattung im Sinne des Art. 5 Abs. 1 Satz 2 GG – worunter auch die Meinungsäußerung fällt.“*

Danach müssten die in der vor der DSGVO (noch) gültigen Datenschutz-Richtlinie vorgesehenen Befreiungen und Ausnahmen zugunsten der Medien nicht nur für Medienunternehmen, sondern für jeden gelten, der bei der konkreten Tätigkeit journalistisch aktiv ist, auch wenn er nicht (haupt-)beruflich als Journalist arbeitet. Denn der Pressebegriff im Rahmen des Medienprivilegs sei rein funktional zu betrachten; es kommt letztlich auf die Zwecke der Publikation an, nicht allein auf die Zugehörigkeit zu Presse oder Rundfunk.

Damit können auch Blogger als Journalisten angesehen werden, wenn sie sich mit Meinungen und Berichten an die Öffentlichkeit wenden und dabei – ähnlich wie die klassischen Medien – einen Beitrag zur Meinungsfreiheit leisten. Hier wird es im Einzelfall darauf ankommen, welche Zielrichtung der Blog verfolgt. Wahrscheinlich werden Tagebuchblogs nicht darunter fallen, weil sie rein privat motiviert sind und nicht relevant für die öffentliche Meinungsbildung.

Welche Tätigkeiten sind journalistisch?

Auch diejenigen, für die prinzipiell das Medienprivileg gilt, können sich nur darauf berufen, wenn sie bei der konkreten Tätigkeit tatsächlich journalistische Zwecke verfolgen. Denn Sinn und Zweck der Privilegierung ist, die Presse unter anderem vor Freigabe ihrer Quellen zu schützen und eine unabhängige Pressearbeit zu gewährleisten. Dies soll dem Schutz des investigativen Journalismus dienen.

Daher sind etwa Recherche, Redaktion, Fotografie, die Veröffentlichung von Berichten und Fotos sowie die Dokumentation und Archivierung personenbezogener Daten zu publizistischen Zwecken umfassend geschützt. Auch Online-Archive von Medien erfüllen journalistische Zwecke, wie Erwägungsgrund 153 zur DSGVO klarstellt.

Die datenschutzrechtliche Privilegierung bezieht sich nicht etwa auf die Personaldatenverarbeitung, die Akquisition von Abonnenten bzw. Kunden oder die Anzeigenverwaltung. Hier gilt ganz normal das Datenschutzrecht. Gemäß BGH soll auch für die kommerzielle Weitergabe von Daten an Dritte keine Privilegierung gelten (Urteil vom 01.02.2011, Az. VI ZR 345/09, Rn. 26).

Danach fällt die Presse- und Öffentlichkeitsarbeit eines Unternehmens bzw. einer Behörde wohl nicht unter journalistisches Arbeiten, weil diese meist primär werblich ist. Anders könnte dies nach der Definition des BVerwG aussehen, wenn es sich um eine nicht werbliche Publikation einer abgegrenzten Abteilung innerhalb eines Unternehmens handelt, die klar journalistischen Zwecken dient. Dieser Punkt ist unter Juristen aber umstritten.

6. Was gilt nach den bisher verabschiedeten und geplanten Regelungen?

6.1 Landesgesetze

Die Länder regeln derzeit die Ausnahmevorschriften für die gedruckte Presse in den Landespressegesetzen (LPG) sowie den Landesdatenschutzgesetzen (LDSG). Regeln etwa zu Online-Zeitungen finden sich in einem speziellen Abschnitt im RStV (siehe unten).

Nordrhein-Westfalen hat in § 12 LPG, welches vor allem auf die klassische (Druck-)Presse Anwendung findet, Folgendes geregelt:

> ***§ 12 Datenschutz***
>
> *Soweit Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen oder literarischen Zwecken von der (…) (Datenschutz-Grundverordnung) (…) außer den Kapiteln I, X und XI nur die Artikel 5 Absatz 1 Buchstabe f in Verbindung mit Absatz 2, Artikel 24 und Artikel 32 Anwendung. Artikel 82 der Verordnung (EU) 2016/679 gilt mit*

der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß der Sätze 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Absatz 1 Buchstabe f, Artikel 24 und Artikel 32 der Verordnung (EU) 2016/679 gehaftet wird.

Das bedeutet, Pressevertreter in **NRW** müssen folgende Regeln der DSGVO beachten:

- Für sie gelten die Kapitel I (Allgemeine Bestimmungen), X und XI (Schlussbestimmungen) der DSGVO.
- Es gilt für sie das **Datengeheimnis**, auf das Journalisten verpflichtet werden müssen (auch **Redaktionsgeheimnis** genannt). Hier bleibt alles wie bisher. Insbesondere dürfen personenbezogene Daten nur für journalistische Zwecke verarbeitet werden. Dabei ist sogar die Weitergabe von Daten an andere Journalisten bzw. Redaktionen erlaubt. Nicht erlaubt ist dies aber etwa zu Werbezwecken.
- Art. 5 Abs. 1 f DSGVO normiert den Grundsatz der Integrität und Vertraulichkeit der Datenverarbeitung, also insbesondere die **Sicherheit der Daten durch entsprechende technische und organisatorische Maßnahmen**. Diese Maßnahmen werden in Art. 24 und Art. 32 DSGVO weiter beschrieben (siehe unten).
- Art. 5 Abs. 2 DSGVO fordert, dass die hierzu ergriffenen **Maßnahmen auch dokumentiert werden (Rechenschaftspflicht)**.
- Art. 82 DSGVO sagt, dass Betroffene **bei einer Verletzung dieser Pflichten die Verantwortlichen verklagen** können, wenn sie sich nicht an die sie betreffenden Regeln zu Organisation und Technik halten. Allerdings sind bislang fast keine entsprechenden Fälle bekannt. Die Frage ist, ob sich das mit der DSGVO ändern wird – da Bürger jetzt sehr viel sensibilisierter sind, was Datenschutz anbelangt. Auch besteht die Gefahr, dass Konkurrenten mithilfe von Abmahnkanzleien entsprechend auch gegen Journalisten vorgehen werden.

Weitestgehend gleichlautend ist § 10 LPG in **Schleswig-Holstein**. Der einzige Unterschied liegt darin, dass das Gesetz nicht von „Beteiligungsunternehmen der Presse“ spricht – was aber letztlich keine große Bedeutung haben dürfte (siehe oben).

In **Mecklenburg-Vorpommern** hingegen müssen die getroffenen Maßnahmen nicht dokumentiert werden, weil der Verweis auf Art. 5 Abs. 2 DSGVO fehlt. Stattdessen gilt mit Art. 33 DSGVO die Verpflichtung, **Datenlecks und Datenpannen der Aufsichtsbehörde zu melden**. Auch dieses Gesetz spricht nur von Unternehmen und Hilfsunternehmen der Presse (siehe oben).

Die weiteren bisher veröffentlichten Gesetzentwürfe der Landespresse- bzw. Landesdatenschutzgesetze in Brandenburg, Bayern, Hessen und Hamburg sehen weitgehend gleichlautende Einschränkungen des Datenschutzes vor.

6.2 Rundfunkstaatsvertrag (RStV)

Auch der Gesetzentwurf zum RStV ist bereits bekannt. Unklar ist nur, ob er bis zum 25. Mai auch von allen Ländern verabschiedet sein wird.

Der RStV enthält zwei Regelungen zum Medienprivileg: § 9 c definiert die Ausnahmen für den klassischen öffentlich-rechtlichen und privaten Rundfunk, also Fernsehen und Radio, § 57 RStV erweitert dieses Medienprivileg auf alle Online-Angebote (Telemedien) der Rundfunkveranstalter wie auch der „Unternehmen und Hilfsunternehmen der Presse." Dass nun auch ausdrücklich Online-Angebote des Rundfunks im RStV geregelt sind, ist neu. Die Regelungen im RStV sind ausführlicher als die der bisher bekannten Landespressegesetze.

Der erste Absatz beider Normen trifft eine fast identische Regelung wie das Landespressegesetz NRW. Ein wichtiger Unterschied in Abs. 1 ist, dass auch Kapitel 8 (Rechtsbehelfe, Haftung und Sanktionen) zunächst allumfassend Anwendung findet. Also **können die Aufsichtsbehörden hier Bußgelder** nach Art. 83 DSGVO verhängen – aber nur bei Verstößen gegen die wenigen anwendbaren datenschutzrechtlichen Normen. Eine wichtige Ausnahme für Online-Angebote sieht § 57 RStV in S. 6 für Telemedien vor: Danach können **keine Bußgelder** verhängt werden, wenn „Unternehmen, Hilfs- und Beteiligungsunternehmen der Presse der Selbstregulierung durch den **Pressekodex** und der Beschwerdeordnung des Deutschen Presserates unterliegen". Das erachten die Länder als notwendig, um die Pressefreiheit angemessen zu berücksichtigen. Die freiwillige Selbstkontrolle sei ein pressespezifisches und mittlerweile bewährtes System inklusive Beschwerderechten, der sich die meisten Presseunternehmen unterworfen haben.

§ 9 c Abs. 2 und § 57 Abs. 3 RStV normieren, dass **Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen sind und dort für dieselbe Zeitdauer aufzubewahren sind wie die Daten selbst**. Auch, wenn Daten übermittelt werden, müssen die Gegendarstellungen & Co. mit übermittelt werden. Hier hat sich im Vergleich zur bisherigen Rechtslage wenig geändert. Es wird nur klargestellt, dass es schon bei der Erhebung von Daten zu Eingriffen in Persönlichkeitsrechte kommen kann, gegen welche die betroffene Person mit Forderungen vorgehen kann.

In § 9 c Abs. 3 und § 57 Abs. 2 RStV ist ein **spezieller medienrechtlicher Auskunftsanspruch** geregelt. Wenn jemand **durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt** wird, kann er Auskunft über die Daten zu seiner Person verlangen, die der Berichterstattung zugrunde liegen. Weiter heißt es dazu:

> *„Allerdings kann die Auskunft nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit*
>
> 1. *aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen mitwirken oder mitgewirkt haben, geschlossen werden kann,*
> 2. *aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,*
> 3. *durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde."*

Nach früherer Rechtslage unterschied sich das Auskunftsrecht des Betroffenen im journalistischen Bereich vom entsprechenden Auskunftsrecht im Rundfunkrecht. Nun wird die Rechtslage angeglichen. Das Auskunftsrecht gilt für Rundfunkanbieter aber erst, wenn tatsächlich über jemanden nach außen hin berichtet wurde und auch nur bei Persönlichkeitsrechtsverletzungen. Eine solche Ausnahme sieht das Gesetz für Online-Angebote nicht vor – hier kann sich der Auskunftsanspruch bereits auf die Recherche oder interne Speicherung von personenbezogenen Daten beziehen.

Des Weiteren enthalten die Normen ein Recht der betroffenen Person auf **Berichtigung** unrichtiger personenbezogener Daten im Datensatz oder die **Hinzufügung einer eigenen Darstellung** von angemessenem Umfang. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist. Dieses Recht ist tatsächlich ähnlich wie in der DSGVO ausgestaltet.

Nur in § 9 c Abs. 4 RStV werden die **öffentlich-rechtlichen Rundfunkanstalten und privatrechtlichen Rundfunkveranstalter** sowie die zu diesen gehörigen Hilfs- oder Beteiligungsunternehmen einer **Aufsicht** über die Einhaltung der geltenden datenschutzrechtlichen Bestimmungen durch Landesrecht unterstellt. Hier wird es eine einheitliche Zuständigkeit eines Rundfunkdatenschutzbeauftragten geben. § 57 RStV enthält keine solche Norm, hier wird also keine Aufsicht stattfinden.

7. Was dürfen Journalisten tun, was andere nicht dürfen?

Bis auf die wenigen rechtlichen Vorgaben, die im Folgenden näher erläutert werden, dürfen Journalisten insbesondere **recherchieren und berichten, wie sie es für richtig halten, ohne an die DSGVO gebunden zu sein**. Sie müssen keine Informationen preisgeben, welche Daten von Dritten sie verarbeiten, sie müssen auf Anfrage von Betroffenen keine Daten löschen etc. Auch hinsichtlich der Vorgaben zum **Datengeheimnis und zur Datensicherheit** müssen sie sich **nicht starr an die Regelungen halten**, denn es ist immer zu berücksichtigen, dass die journalistische Arbeit nicht gefährdet werden darf (siehe unten).

Zwiegespalten sieht es bei den Regelungen für **Webseiten** aus. Wenn die Verarbeitung von Daten einer Webseite (z. B. Nutzerdaten wie die IP-Adresse) journalistischen Zwecken dient, dann gilt das Medienprivileg. Werden Nutzerdaten aber ohne journalistische Zwecke oder sogar aus reinen Marketing-Gesichtspunkten verarbeitet, sollte man sich diesbezüglich an die DSGVO halten. Letztlich muss hier im Einzelfall geschaut werden, welche Regelungen Anwendung finden. Diese Aspekte spiegeln sich dann auch in der Datenschutzerklärung wider: Datenverarbeitungen zu journalistischen Zwecken dürfen „geheim“ bleiben, während zum Beispiel über das Tracking zu Marketing-Zwecken in der Datenschutzerklärung informiert werden muss (siehe unten).

Wie schon zuvor sind die datenschutzrechtlichen **Aufsichtsbehörden** grundsätzlich nicht für Journalisten zuständig. Lediglich Rundfunkveranstalter sind nach dem geplanten RStV einer speziellen datenschutzrechtlichen Aufsicht in Form eines Rundfunkdatenschutzbeauftragten unterworfen.

Die Landesgesetze für die gedruckte Presse sehen auch keine **Bußgelder** für Journalisten vor. Allerdings können die Aufsichtsbehörden solche Bußgelder gegen Rundfunkveranstalter sowie Online-Angebote verhängen. Online-Angebote hingegen sind davon wiederum ausgenommen, wenn sie sich freiwillig dem Pressekodex des Deutschen Presserates unterworfen haben.

Grundsätzlich müssen Journalisten auch keine **Auskunft** über verarbeitete Daten geben. Doch sehen manche Landesgesetze sowie der RStV spezielle Auskunftsansprüche gegen Journalisten vor. Diese gelten aber nicht, wenn sich die Presse- oder Online-Redaktion dem Pressekodex unterworfen hat. Rundfunkanstalten hingegen können sich dem gesetzlichen Auskunftsanspruch nicht entziehen.

Weitergehende **Einschränkungen** ergeben sich nur dann, wenn sich Journalisten freiwillig den Regelungen des Pressekodex des Deutschen Presserates unterworfen haben.

8. Sonderfall Fotorecht

Im Bereich der Fotografie gibt es – unabhängig vom Medienprivileg – ein spezielleres Gesetz als das BDSG, nämlich das Kunsturhebergesetz (KUG). Dieses Gesetz stellt in §§ 22, 23 besondere Regeln für das „Recht am eigenen Bild“ als Teil des Allgemeinen Persönlichkeitsrechts auf. Diese gelten grundsätzlich nur für die Veröffentlichung von Personenfotos, nicht aber für deren Aufnahme.

§ 22 KUG erlaubt die Verbreitung bzw. öffentliche Zurschaustellung von Personenfotos grundsätzlich nur mit Einwilligung – es sei denn, es gilt eine der gesetzlichen Ausnahmen aus § 23 KUG. Hiernach sind Veröffentlichungen von Fotos, die im Zusammenhang mit einem zeitgeschichtlichen Ereignis stehen, sowie Fotos von Versammlungen oder Landschaften, auf denen Personen als „Beiwerk“ zu sehen sind, in der Regel auch ohne Einwilligung der abgebildeten Personen erlaubt.

Bisher hat die Rechtsprechung angenommen, dass das BDSG auf die Aufnahme einer Fotografie selbst nicht angewendet werden soll. So wird eine Fotoaufnahme nur dann als mögliche Rechtsverletzung angesehen, wenn eine Güter- und Interessenabwägung mit dem Persönlichkeitsrecht des Fotografierten im jeweiligen Einzelfall gegen die Aufnahme spricht. Das ist insbesondere der Fall, wenn jede denkbare Veröffentlichung oder Verbreitung von vornherein ohne Einwilligung der abgebildeten Person unzulässig wäre. Letztlich waren bisher also die Grundsätze, die für die Veröffentlichung eines Fotos galten, auch für die Aufnahme selbst relevant.

In den vergangenen Wochen sind hitzige Diskussionen um die Anwendbarkeit des KUG im Rahmen der DSGVO entbrannt: Befürchtet wurde das Ende der Fotografie. Klar ist jedoch: Journalisten sind von der DSGVO auch im Rahmen des Fotorechts ausgenommen. Für sie gelten weiterhin die alten Regelungen – sowohl für die Aufnahme eines Fotos als auch für dessen Veröffentlichung. Lediglich gewerblich tätige Fotografen, die bei der Anfertigung des Fotos nicht zu journalistischen Zwecken handeln, müssen diesbezüglich die DSGVO beachten. Doch nach einer Stellungnahme des Bundesinnenministeriums dürfte auch für sie im Rahmen der Veröffentlichung weiterhin das KUG anwendbar sein. Diese Diskrepanz könnte in der Praxis noch zu erheblichen

Problemen führen, die Journalisten aber nicht betreffen. Denn sobald ein Foto in ihrem Bereich zu journalistischen Zwecken gespeichert, bearbeitet oder veröffentlicht wird, gilt das Medienprivileg.

9. Was werden die Gerichte zu den landesrechtlichen Regelungen sagen?

Die Tatsache, dass die meisten bisher bekannten Gesetze wie bisher nur die Anwendbarkeit der DSGVO weitgehend ausschließen und nicht weitergehend differenziert wird, wird von vielen Juristen kritisiert. Klar ist, dass die Gesetzgeber versuchen, den Status quo des Medienprivilegs beizubehalten. Das ist an sich erst einmal wünschenswert.

Doch es wäre möglich, dass diese Gesetze europarechtswidrig sind. Denn die Öffnungsklausel in Art. 85 DSGVO, die den Ländern eine entsprechende Gesetzgebung erlaubt, spricht davon, dass die DSGVO nur soweit eingeschränkt werden darf, wie es *„erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung der Informationsfreiheit in Einklang zu bringen.“* Es könnte also sein, dass der pauschale Ausschluss der DSGVO gar nicht erforderlich ist, um die Grundrechte zu gewährleisten. Auch die Gerichte könnten die Ansicht vertreten, dass eine differenziertere Grundrechtsabwägung hätte vorgenommen werden müssen. Es ist also unklar, ob diese Regelungen aus europarechtlicher Sicht auch Bestand haben werden. Bis die Rechtsprechung hier klärend wirkt, müssen sich Journalisten nur an das geltende Recht halten.

Der Vorteil der weitgehenden Beibehaltung des bisherigen Medienprivilegs: Es ist davon auszugehen, dass weiterhin auf die bisherige Rechtsprechung zum Presse- bzw. Rundfunkbegriff sowie zum Medienprivileg zurückgegriffen werden kann. Für die journalistische Arbeit bedeutet das also mit hoher Wahrscheinlichkeit fast keine Änderung.

10.Für journalistische Tätigkeiten anwendbare Regelungen der DSGVO

10.1 Geeignete technische und organisatorische Maßnahmen (TOM)

Die DSGVO stellt auch Anforderungen an die Technik und die interne Organisation einer Redaktion bzw. an den Arbeitsplatz eines selbstständigen Journalisten (Verantwortliche).

Verantwortliche müssen nach Art. 24 DSGVO konkret geeignete **technische und organisatorische Maßnahmen (TOM)** treffen, um die **Einhaltung des Datenschutzgrundsatzes der „Integrität und Vertraulichkeit“** zu gewährleisten. Dieser lautet nach Art. 5 Abs. 1 f:

> Daten müssen *„in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).*

Welche Maßnahmen konkret erforderlich sind, hängt darüber hinaus von der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen

Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen ab (Art. 24 Abs. 1 DSGVO).

Art. 32 DSGVO erweitert dann die Maßgaben für die technisch-organisatorischen Maßnahmen:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche (…) geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."*

Dabei müssen die Maßnahmen in einem wirtschaftlich angemessenen Verhältnis zum Schutzbedarf der verarbeiteten personenbezogenen Daten stehen. Das Gesetz nennt in Artikel 32 Absatz 1 DSGVO als wichtige, aber nicht abschließende Vorgaben folgende Maßnahmen:

- *„die Pseudonymisierung und Verschlüsselung personenbezogener Daten;*
- *die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen*
- *die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen*
- *ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung."*

Bei der Frage, welche Sicherheitsvorkehrungen konkret erforderlich sind, heißt es etwa in der bayerischen Begründung zum RStV:

> *„Dieser Verweis soll aber nicht dazu führen, dass über die Anforderung, ‚dass die Verarbeitung gemäß dieser Verordnung erfolgt', ‚durch die Hintertür' der gesamte Pflichtenkanon der Verordnung Anwendung findet. Vielmehr handelt es sich um einen Rückverweis auf die gesamte Verordnung einschließlich Art. 85, mithin auf das geltende System. Zu berücksichtigen sind dabei insbesondere die Zwecke der Verarbeitung, was auch die journalistischen Zwecke berücksichtigungsfähig macht."*

Letztlich dürfen die Vorgaben zur Datensicherheit also keinesfalls die journalistische Arbeit einschränken, sodass jeder Presseverteter prüfen muss, was im Einzelfall sinnvoll ist.

Deswegen sind die **gesetzlichen Vorgaben nicht starr einzuhalten**. Gerade die Pseudonymisierung der Daten wird wohl nicht zwingend nötig wein, weil sonst die Pressearbeit eingeschränkt werden könnte. Letztlich ist dies wohl nur eine mögliche, keinesfalls aber eine zwingende Maßnahme. Daten sollen nur dann pseudonymisiert werden, wenn es die journalistische Arbeit nicht beeinträchtigt.

Weitere **Maßnahmen, die nötig sein können, um die Datensicherheit und das Datengeheimnis zu gewährleisten**, sind:

- Redaktionsgeheimnis wahren (siehe oben) und Mitarbeiter schriftlich auf das Redaktionsgeheimnis verpflichten;
- ein gutes Sicherheitskonzept in Bezug auf Technik und Organisation in den Büros einrichten, sodass Daten nicht an Dritte gelangen. Dazu gehören zum Beispiel:
    - sichere, regelmäßig erneuerte Passwörter;
    - Verschlüsselungen insbesondere bei E-Mails und anderen Kommunikationswegen;
    - prüfen, ob die Daten in einer Cloud wirklich sicher sind. Hier können die (für Journalisten nicht anwendbaren) Regeln zur Auftragsverarbeitung helfen. Gewählt werden sollten nur solche Anbieter, die sich an die DSGVO halten und entsprechend zertifiziert sind. Anbieter mit Sitz außerhalb der EU sollten als sicher anerkannt sein; zum Beispiel US-Firmen nach dem EU-Abkommen mit den USA (Privacy Shield). Eine entsprechende Zertifizierung haben zum Beispiel Dropbox oder Mailchimp.
    - sensible Unterlagen wegschließen, Räume verschließen, Computer abends einschließen etc.;
    - ein geeigneter Virenschutz mit regelmäßigen Updates;
    - Anweisungen der Redaktionsleitung an die Beschäftigten – etwa eine Richtlinie zur Datensicherheit;
- eine SSL-Verschlüsselung der eigenen Internetseite ist empfehlenswert;
- im Netz mit verdeckter IP-Adresse surfen;
- ein Notfallplan bei Datenlecks.

Bei allem aber gilt: **Die journalistische Freiheit kann im Einzelfall Vorrang haben.** Sollte es technisch zu aufwendig sein, Daten zu verschlüsseln oder zu pseudonymisieren, und sollte die journalistische Arbeit dadurch gefährdet sein (sollte es besonders schnell gehen müssen), dann können Abstriche beim Datenschutz gemacht werden.

10.2 Melde- und Informationspflichten bei Datenpannen (Mecklenburg-Vorpommern)

Für Pressevertreter, die in Mecklenburg-Vorpommern tätig werden, gelten zukünftig die Vorgaben von Art. 33 DSGVO. Danach müssen grundsätzlich alle Verletzungen des Schutzes personenbezogener Daten gemeldet werden, es sei denn, das Risiko für persönliche Rechte und Freiheiten ist unwahrscheinlich.

Verantwortliche müssen solche Vorfälle (Incidents) der Aufsichtsbehörde unverzüglich und möglichst **binnen 72 Stunden** nach Bekanntwerden der Verletzung melden. Dabei sind gemäß Art. 33 Abs. 3 DSGVO zumindest **folgende Informationen zu übermitteln**:

- Beschreibung des Vorfalls, Angabe der Kategorie der betroffenen Daten, Anzahl der Betroffenen und betroffenen Datensätze;
- Name und Kontaktdaten des Datenschutzbeauftragten oder eines anderen informierten Ansprechpartners;
- Beschreibung der Folgen der Datenschutzverletzung;
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

11.Regelungen der DSGVO, die für nicht-journalistische Tätigkeiten gelten

Es gibt zahlreiche Bereiche, in denen das Medienprivileg nicht gilt, weil die Tätigkeit nicht journalistischen Zwecken dient. Wer zum Beispiel eine Website betreibt, selbst ein Medienunternehmen leitet oder auf andere Weise neben der rein journalistischen Tätigkeit auch unternehmerisch tätig ist, der muss – auch als Journalist – die klassischen Pflichten aller datenschutzrechtlichen Verantwortlichen beachten. Nicht-journalistische Tätigkeiten sind insbesondere:

- die Speicherung von Bewerber- und Mitarbeiterdaten sowie Daten freier Journalisten;
- Akquisition von Abonnenten bzw. Kunden;
- Anzeigenverwaltung;
- ein rein werblicher Newsletter und sonstige rein werbliche Aktivitäten;*
- kommerzielle Weitergabe von Daten an Dritte;*
- berufsfremde Tätigkeiten von Journalisten, zum Beispiel als Referenten, Dozenten, Berater, Übersetzer etc.

* Es kann Tätigkeiten geben, die im Einzelfall journalistischen Zwecken dienen, in anderen Fällen jedoch rein kommerziell sind (z. B. PR, Newsletter, Datenweitergabe an Dritte).

11.1. Wann dürfen personenbezogene Daten überhaupt verarbeitet werden?

Die Verarbeitung von personenbezogenen Daten ist nach der DSGVO nur dann rechtmäßig, wenn eine Einwilligung der betroffenen Person oder eine andere, insbesondere in Art. 6 DSGVO normierte Ausnahme vorliegt (Verbot mit Erlaubnisvorbehalt). In der Datenschutzerklärung ist außerdem die Rechtsgrundlage anzugeben, auf die sich eine Datenverarbeitung stützt. Die praktisch relevantesten Erlaubnistatbestände nach Art. 6 DSGVO sind:

- **Einwilligung** des Betroffenen, die den Anforderungen der Art. 7, 8 DSGVO entspricht (Art. 6 Abs. 1 Satz 1 lit. a DSGVO);
- Erforderlichkeit für die **Erfüllung eines Vertrags** oder zur Durchführung **vorvertraglicher Maßnahmen**, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 Satz 1 lit. b DSGVO);
- Erforderlichkeit zur Wahrung der **berechtigten Interessen** des Verantwortlichen oder eines Dritten, wenn keine schutzwürdigen Interessen des Betroffenen überwiegen (Art. 6 Abs. 1 Satz 1 lit. f DSGVO).

Einwilligung

Eine Einwilligung ist nach Art. 4 Nr. 11 DSGVO

> *„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“*

Bei der Einholung einer Einwilligung der betroffenen Person sind folgende Voraussetzungen zu beachten:

- Die Einwilligung muss sich auf einen **bestimmten Fall** (Art. 4 Nr. 11 DSGVO, keine *„Pauschaleinwilligung“*) und auf einen **bestimmten Verarbeitungszweck** beziehen (Art. 6 Abs. 1 Satz 1 lit. a DSGVO).
- Die Einwilligung muss **freiwillig** erteilt werden. Der Einwilligende muss eine echte und freie Wahl haben und in der Lage sein, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (Art. 4 Nr. 11, 7 Abs. 4 DSGVO). Der Betroffene muss also ausreichend über die Reichweite der Einwilligung **informiert** gewesen sein, insbesondere auch über die **Zwecke der Datenverarbeitung**. Außerdem ist hier das neue ***„Kopplungsverbot“*** zu beachten (Art. 7 Abs. 4 DSGVO): Es ist zwar juristisch umstritten, wie weit es wirklich greift, sicherheitshalber sollte aber zukünftig eine Vertragserfüllung, zum Beispiel eine Gratisleistung, nicht mehr von einer Einwilligung in die werbliche Datenverarbeitung abhängig gemacht werden.
- Der Verantwortliche muss das Vorliegen einer Einwilligungserklärung **nachweisen** können (Art. 7 Abs. 1 DSGVO).
- Der Einwilligungstext muss **klar formuliert** sein.
- Der Text muss **gut zugänglich** sein (Art. 7 Abs. 2 DSGVO).
- Es ist deutlich auf die **Widerrufsmöglichkeit** hinzuweisen (Art. 7 Abs. 3 Satz 3 DSGVO).
- Zu beachten ist, dass in Art. 8 DSGVO die Bedingungen für die Einwilligung eines Kindes gesondert geregelt sind. Diese steht bis zum vollendeten **16. Lebensjahr** steht unter dem Vorbehalt der Zustimmung seiner gesetzlichen Vertreter.

Gelten die bisher eingeholten Einwilligungen weiterhin?

In der Vergangenheit eingeholte Einwilligungen müssen den **Grundsätzen der neuen DSGVO entsprechen**. Tun sie dies nicht, sind sie erneut einzuholen. Doch **bestehende Einwilligungen müssen in der Regel nicht neu eingeholt werden**, wenn sie bislang geltendem Recht entsprechen. Die einzige Problematik könnte dann auftreten, wenn die bereits eingeholte Einwilligung in die Datenverarbeitung an andere Erklärungen gekoppelt war – hier besteht Rechtsunsicherheit (siehe oben).

Erfüllung eines Vertrages

Die Verarbeitung personenbezogener Daten von Kunden oder anderen Vertragspartnern ist nicht selten bereits zur Erfüllung eines Vertrags erforderlich und damit gesetzlich erlaubt. Es kommt im Einzelfall auf den konkret abgeschlossenen Vertrag und die hieraus resultierenden Pflichten an, wann welche Daten auf Grundlage dieser Erlaubnisnorm verarbeitet werden dürfen. Zu beachten sind jedoch die Grundsätze der Datenminimierung und der Zweckbindung: Verarbeitet werden sollten nur Daten, die wirklich für die Vertragserfüllung notwendig sind.

Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen

Hierunter fallen alle Informationen, die vor dem Abschluss eines Vertrages ausgetauscht werden, zum Beispiel, wenn Interessenten mehr Informationen über Leistungen anfragen, wenn ein Kostenvoranschlag erstellt oder die Kreditwürdigkeit potenzieller Kunden überprüft wird. Die

Daten dürfen aber nur so lange gespeichert werden, wie noch nicht klar ist, dass der Vertrag auch zustande kommt. Hat der Interessent abgesagt, sind die gespeicherten Daten zu **löschen**.

Berechtigtes Interesse

Diese Erlaubnisnorm wird in Zukunft besonders wichtig werden. Sie ermöglicht die Datenverarbeitung ohne Einwilligung der Betroffenen, wenn eine **ausführliche Interessenabwägung** im Einzelfall zugunsten des Verarbeiters ausfällt. Unter einem *„berechtigten Interesse“* versteht man das **rechtliche, tatsächliche, wirtschaftliche oder ideelle Interesse, das von der Rechtsordnung anerkannt wird**. Wenn klar ist, welcher Zweck mit der Verarbeitung verfolgt wird, ist zu prüfen, ob die Interessen bzw. Grundrechte und EU-Grundfreiheiten des Betroffenen auf Schutz seiner personenbezogenen Daten weniger Gewicht haben als das Eigeninteresse des Verarbeiters. Diese Interessenabwägung ist für jede einzelne Datenverarbeitung gesondert vorzunehmen, bei der diese Erlaubnis gelten soll. Diese Interessenabwägung sollte auch intern dokumentiert werden.

Näheres zum berechtigten Interesse findet sich im *„Erwägungsgrund 47“* zur DSGVO. Danach ist vor allem zu prüfen,

> *„ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.“*

Wenn also jedem klar ist, dass die Daten so, wie sie verarbeitet werden, auch üblicherweise genutzt werden, spricht das für das überwiegende berechtigte Interesse des Verarbeiters.

Ein berechtigtes Interesse an der Verarbeitung personenbezogener Daten besteht gemäß Erwägungsgrund bei **Kunden** oder **Mitarbeitern** des Verarbeiters, aber auch bei **Direktwerbung**. Es ist aber juristisch nicht eindeutig geklärt, welche Form der Direktwerbung danach erlaubt sein kann und welche nicht. Daher sollte man sich nicht darauf stützen, wenn man etwa per Kaltakquise potenzielle Neukunden anspricht. Allerdings spricht vieles dafür, dass die E-Mail-Werbung ohne eine Einwilligung zumindest bei **Bestandskunden** in Grenzen zulässig ist. So ist dies auch im weiterhin geltenden Wettbewerbsrecht geregelt.

Bei Berufung auf das Wettbewerbsrecht sind die Betroffenen verständlich und umfassend über die geplante Datenverarbeitung zu informieren und auf ihr **Widerspruchsrecht** hinzuweisen.

Wann dürfen Daten von Mitarbeitern gespeichert werden?

Die Daten von Mitarbeiter dürfen gespeichert werden, sofern dies **für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich** ist (§ 26 Abs. 1 S. 1 BDSG in der Fassung ab 25. Mai 2018). Wann dies der Fall ist, muss immer anhand der Umstände des Einzelfalls bestimmt werden. Dabei kommt es auf eine Abwägung zwischen den Arbeitgeber- und Arbeitnehmerinteressen an. Auch die Speicherung auf Grundlage von **Kollektivvereinbarungen** ist zulässig, sofern hier angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person (Art. 88 Abs. 2 DSGVO) getroffen wurden. Problematisch ist, dass diese

gesetzlichen Erlaubnistatbestände recht schwammig formuliert sind und Rechtsunsicherheit besteht.

Zusätzlich eine **Einwilligung des Arbeitnehmers** einzuholen wird in den meisten Fällen vor Gericht keinen Bestand haben. Solange es nämlich um das konkrete Arbeitsverhältnis geht, besteht eine Abhängigkeit zwischen Arbeitgeber und Arbeitnehmer, sodass eine erteilte Einwilligung im Zweifel nicht als freiwillig gilt. Lediglich bei gewissen Vereinbarungen betreffend Zusatzleistungen (z. B Nutzung eines Diensthandys oder Aufnahme in die Geburtstagsliste) dürften Einwilligungen wirksam sein. Daher gilt: **Möglichst nur so wenige Daten von Mitarbeitern verarbeiten wie absolut notwendig.**

11.2. Informationspflichten

Art. 13 und 14 DSGVO sehen für Verantwortliche umfangreiche Informationspflichten Betroffenen gegenüber vor. Dabei ist auf eine präzise, transparente, verständliche und leicht zugängliche Form sowie eine klare und einfache Sprache zu achten (Art. 12 Abs. 1 DSGVO). Die Informationspflichten bestehen sowohl online (z. B. in der Datenschutzerklärung) als auch offline, etwa für Besucher vor Ort. Diese erweiterten Pflichten sollen den Datenschutz im Vergleich zu den aktuell geltenden Regelungen des BDSG stärken.

Dabei unterteilt die DSGVO die Informationspflichten, je nachdem, ob personenbezogene Daten direkt beim Betroffenen erhoben (Art. 13 DSGVO) oder von Dritten (also nicht bei der betroffenen Person selbst) bezogen werden (Art. 14 DSGVO).

Werden Daten **direkt beim Betroffenen erhoben**, müssen folgende Informationen **nach Art. 13 Abs. 1 DSGVO mitgeteilt werden:**

- Name und Kontaktdaten des Verantwortlichen;
- ggf. Kontaktdaten des Datenschutzbeauftragten (DSB);
- Zwecke der Datenverarbeitung;
- Rechtsgrundlage der Datenverarbeitung;
- Darstellung der berechtigten Interessen (wenn die Datenverarbeitung auf dem Tatbestand der Interessenabwägung gem. Art. 6 Abs. 1 f DSGVO beruht);
- ggf. Empfänger oder Kategorien von Empfängern der Daten;
- ggf. Informationen zur Datenübermittlung in Drittländer.

Nach **Art. 13 Abs. 2 DSGVO** müssen folgende weitere Informationen **zur Verfügung gestellt werden**, um eine faire und transparente Datenverarbeitung zu gewährleisten:

- Dauer der Datenspeicherung – wenn nicht möglich, Kriterien für die Festlegung der Dauer;
- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht bei besonderer Situation, Datenportabilität und Beschwerderecht zur Aufsichtsbehörde);
- wenn die Datenverarbeitung auf einer Einwilligung beruht: Hinweis auf das Recht zum jederzeitigen Widerruf;

- Grundlage der Bereitstellung der Daten auf gesetzlicher oder vertraglicher Basis und Folgen der Nichtbereitstellung;
- Bestehen einer automatisierten Einzelfallentscheidung einschließlich Profiling (z. B. das Erstellen eines umfassenden Nutzerprofils oder die Bildung von sogenannten Scorewerten durch Verknüpfen, Speichern, Auswerten und Zusammenlegen von verschiedenen Daten zu einer Person);
- die Information darüber, ob die Datenverarbeitung gesetzlich bzw. vertraglich vorgeschrieben bzw. für einen Vertragsschluss erforderlich ist.

Werden Daten von Dritten bezogen (z. B. durch Übermittlung) und nicht direkt beim Betroffenen erhoben, gelten nach **Art. 14 DSGVO** leicht abgewandelte Informationspflichten:

- Nach Art. 14 Abs. 1 DSGVO müssen im Wesentlichen die gleichen Informationen mitgeteilt werden wie bei der Direkterhebung. Weil der Betroffene aber keine Kenntnis von der weiteren Verarbeitung hat, muss ihm zusätzlich mitgeteilt werden, welche Kategorien von personenbezogenen Daten verarbeitet werden.
- Nach Art. 14 Abs. 2 DSGVO muss die Datenquelle und auch die Information angegeben werden.

Werden die Daten **direkt beim Betroffenen** erhoben, müssen die Informationen gem. Art. 13 DSGVO zum **Zeitpunkt** der Erhebung der personenbezogenen Daten mitgeteilt bzw. zur Verfügung gestellt werden. Bei der **weiteren Verarbeitung der Daten durch Dritte** kann die Information nach Art. 14 DSGVO auch später erfolgen. Der Verantwortliche muss die Informationen nachträglich innerhalb einer angemessenen Frist nach Erlangung der Daten mitteilen. Diese Frist ist abhängig von den spezifischen Umständen, darf aber maximal einen Monat betragen.

Von den Informationspflichten gelten einige **Ausnahmen**. So hat der Betroffene keinen Informationsanspruch, wenn die Informationserteilung einen unverhältnismäßig hohen Aufwand darstellt, unmöglich ist oder voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. In diesem Fall ist eine öffentliche Bekanntmachung dieser Information, zum Beispiel auf einer Webseite, erforderlich.

11.3. Die Datenschutzerklärung anpassen

Grundsätzlich muss **jeder Webseitenbetreiber** eine Datenschutzerklärung bereithalten, damit für die Besucher deutlich wird, welche Daten wie und wozu erhoben werden. Diese Datenschutzerklärung muss Antworten auf folgende Fragen geben können:

- Welche personenbezogenen Daten werden erhoben (z. B. die IP-Adresse eines Besuchers)?
- Was passiert mit den erhobenen Daten?
- Warum werden überhaupt Daten erhoben?
- Werden die erhobenen Daten an Dritte weitergegeben?
- Findet ein grenzüberschreitender Datenverkehr statt?
- Welche Maßnahmen werden zur Gewährleistung der Sicherheit der Daten ergriffen?

Mit Geltung der DSGVO müssen Webseitenbetreiber neue Anforderungen an die Datenschutzerklärung beachten. Da damit eigentlich keine der bisherigen Datenschutzerklärungen den Anforderungen der DSGVO entspricht, sollte jeder, der eine Webseite betreibt, seine Datenschutzerklärung **dringend an die DSGVO** anpassen. Diese fordert zukünftig, dass in der Datenschutzerklärung folgende Informationen enthalten sind:

- alle in Art. 13 und 14 DSGVO genannten Pflichtinformationen (siehe oben);
- Erläuterung des Datenerhebungs- bzw. -verarbeitungsvorgangs und des dahinterstehenden Zwecks;
- die konkret anwendbare Rechtsgrundlage;
- nicht mehr zwingend notwendig, aber empfehlenswert: Information über Art und Umfang der Verarbeitung in der Datenschutzerklärung belassen;
- Hinweis auf ein (eingeschränktes) Widerspruchsrecht, wenn die Verarbeitung personenbezogener Daten auf Art. 6 Abs. 1 e oder f DSGVO beruht;
- Hinweis auf ein Widerspruchsrecht gegen zulässige Direktwerbung und – in besonders schutzwürdigen Fällen – auch gegen sonstige zulässige Datenverarbeitungen. Da die Information hierüber laut Gesetz separat zu erfolgen hat, ist noch unklar, ob dies überhaupt Teil der Datenschutzerklärung sein soll.

Neben den zwingend erforderlichen müssen Sie im Einzelfall weitere Informationen vorhalten:

- Hinweis auf Widerrufsrecht, wenn die Verarbeitung personenbezogener Daten auf einer Einwilligung der betroffenen Person beruht (Art. 7 DSGVO);
- sofern vorhanden: Kontaktdaten des Datenschutzbeauftragten;
- bei gesetzlicher oder vertraglicher Pflicht zur Datenerhebung: Aufklärung des Betroffenen über diese Pflicht und die möglichen Folgen einer Nichtbereitstellung;
- beim Einsatz automatisierter Entscheidungsfindungen (inklusive Profiling): Aufklärung hierüber, insbesondere über die zugrunde liegende Logik, die Tragweite und die angestrebten Auswirkungen für den Betroffenen;
- bei einer Weitergabe an Dritte: Angabe der Empfänger/der Kategorie von Empfängern;
- Angabe der Absicht zur Datenübermittlung ins Ausland (dann auch Angabe des von der EU-Kommission festgelegten Datenschutzniveaus des jeweiligen Drittlandes);
- im Fall von Übermittlungen nach Art. 46, 47 oder 49 DSGVO: Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist oder wo sie verfügbar sind.

Hierzu können Sie in einem ersten Schritt auch unseren individualisierbaren Online-Datenschutzerklärungs-Generator nutzen, den wir von der Kanzlei WILDE BEUGER SOLMECKE gemeinsam mit der Deutschen Gesellschaft für Datenschutz (DGD) entwickelt haben: https://www.wbs-law.de/it-recht/datenschutzrecht/datenschutzerklaerung-generator/ Allerdings sollten Sie für den Fall, dass auf Ihrer Webseite zumindest auch zu journalistischen Zwecken Daten verarbeitet werden, die Erklärung von einem auf das Presserecht spezialisierten Anwalt prüfen lassen.

11.4. Auf Auskunftsansprüche Betroffener reagieren

Die Betroffenen haben gemäß Art. 15 DSGVO ein **umfassendes Auskunftsrecht**. Es ist weitestgehend mit dem bisherigen § 34 BDSG vergleichbar – neu ist jedoch, dass der Betroffene nun auch eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, verlangen kann.

Der Verantwortliche muss auf Verlangen der betroffenen Person eine Bestätigung darüber erteilen, ob er überhaupt personenbezogene Daten verarbeitet. Sofern dies der Fall ist, hat die betroffene Person das Recht auf weitergehende Auskunft im Hinblick auf die in Art. 15 Abs. 1 lit. a – h DSGVO genannten Informationen: Dies betrifft die Verarbeitungszwecke, die Kategorien personenbezogener Daten, die verarbeitet werden, und die Herkunft der Daten.

Der Verantwortliche muss die in Art. 15 DSGVO genannten Informationen „unverzüglich" zur Verfügung stellen. Dies ist in der Regel spätestens ein Monat nach der Anfrage; nur in Ausnahmefällen kann die Frist zwei Monate betragen (Art. 12 Abs. 3 DSGVO).

Die meisten Juristen gehen mit der DSGVO davon aus, dass der Anspruch höchstpersönlich und nur selbst geltend zu machen ist – oder zumindest eine entsprechende Vollmacht des Betroffenen erfordert.

11.5. Auf Löschungsansprüche Betroffener reagieren

Art. 17 DSGVO gibt Betroffenen qua Gesetz ein „Recht auf Vergessenwerden". Der Gedanke, dass personenbezogene Daten gelöscht werden müssen, ist allerdings nicht neu. Das **Recht auf Löschung** der eigenen Daten besteht in diesen Fällen:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit a DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein (Art. 21 Abs. 2 DSGVO) ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor (Art. 21 Abs. 1 DSGVO).
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der EU-Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Das Recht auf Vergessenwerden findet nach Artikel 17 Abs. 3 DSGVO allerdings **keine Anwendung**, wenn zum Beispiel:

- die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist;
- die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist;
- die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 DSGVO erforderlich ist, soweit das in Abs. 1 genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Bislang hatte es zu diesem Punkt lediglich Gerichtsentscheidungen gegeben. Die Umsetzung der Löschpflicht war in großen Teilen unklar. Die neue Norm sieht hierzu eine detaillierte Prozedur vor.
Daneben ist in Art. 16 DSGVO ein „**Recht auf Berichtigung**“ geregelt. Danach können Betroffene verlangen, dass unrichtige personenbezogene Daten berichtigt und – unter Berücksichtigung der Verarbeitungszwecke – unvollständige personenbezogene Daten vervollständigt werden.

Schließlich regelt Art. 18 DSGVO das Recht auf Einschränkung der Verarbeitung. Danach hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung unter gewissen Voraussetzungen (Art. 18 Abs. 1 lit. a – d DSGVO) zu verlangen.

11.6. Auftragsverarbeiter überprüfen und Verträge anpassen

Auftragsverarbeiter kann gemäß Art. 4 Nr. 8 DSGVO sein:

> *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“*

Das Verhältnis, das zwischen externem Dienstleister und Auftraggeber besteht, nennt man aus datenschutzrechtlicher Sicht „Auftragsverarbeitung“. Die Auftragsverarbeitung ist in Art. 28, 29 DSGVO geregelt. Beispiele für Auftragsverarbeiter sind etwa: Einschaltung externer Wartungsdienstleister und sonstige EDV-, Telekommunikations- oder IT-Dienstleister mit Fernzugriff auf Daten, externe Rechenzentren, E-Mail-Provider, Cloud-Anbieter (wie Google Drive oder Dropbox), externe Lohnbuchhaltungsbüros, Callcenter zur Kundenbetreuung, externe Agenturen zur Durchführung von Marketingaktionen. Schließlich ist sogar der Abfallentsorger als Auftragsverarbeiter anzusehen, wenn er Zugriff auf entsorgte Papiere hat, die personenbezogene Daten enthalten.

Keine Auftragsverarbeiter, sondern Verantwortliche sind eigenständig agierende Berufsgruppen, zum Beispiel Berufsgeheimnisträger wie etwa Steuerberater, Wirtschaftsprüfer und Rechtsanwälte, Bankinstitute für Überweisungen oder die Post für ihre Dienstleistungen. Auch gemeinsam für eine Verarbeitung Verantwortliche (Art. 26 DSGVO) fallen nicht unter den Begriff.

Auftragsverarbeiter werden künftig stärker in die Pflicht genommen, die Einhaltung der Datenschutzregelungen einzuhalten. Sie müssen künftig ein Verarbeitungsverzeichnis erstellen (Art. 30 Abs. 2 DSGVO), mit der Datenschutzaufsicht zusammenarbeiten (Art. 31 DSGVO), die

technischen und organisatorischen Maßnahmen der Datensicherheit einhalten (Art. 32 Abs. 1 DSGVO) oder auch die Beschränkungen für den Datentransfer in Drittländer beachten (Art. 44 DSGVO).

Verantwortliche müssen zunächst prüfen, wer für sie personenbezogene Daten Dritter verarbeitet. Anschließend müssen sie sicherstellen, dass sie gemäß Art. 28 DSGVO nur mit Auftragsverarbeitern arbeiten,

> *„die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet."*

Dabei müssen sie vor allem auf **die Auswahl, die vertragliche Ausgestaltung und die anschließende Kontrolle Ihrer externen Dienstleister achten**. Hat ein Unternehmen noch keine Verträge mit externen Dienstleistern geschlossen, sollte dies dringend nachgeholt werden. Bestehende Verträge sind zu überprüfen und im Sinne der DSGVO anpassen. Werden hier Fehler gemacht, drohen Bußgelder.

Bislang waren die Auftraggeber Betroffenen gegenüber allein verantwortlich für etwaige Schäden bei der Datenverarbeitung. Art. 82 DSGVO sieht nun eine gemeinsame Haftung des Auftragsverarbeiters und des Auftraggebers gegenüber den Betroffenen vor. Das bedeutet, ein Geschädigter kann von jedem die volle Summe verlangen. Untereinander hängt die Schadensersatzpflicht aber davon ab, wessen Verschuldensbeitrag schwerer wiegt. Derjenige, der die volle Summe hat zahlen müssen, kann sich einen entsprechenden Anteil vom anderen zurückholen.

11.7. Datenschutzfolgenabschätzung vornehmen?

Mit der in Art. 35 DSGVO normierten Datenschutzfolgeabschätzung (DSFA) müssen Verantwortliche einschätzen, ob die jeweilige Verarbeitung voraussichtlich hohe Risiken für die Rechte oder Freiheiten des Betroffenen ausweist. Sie erfolgt in bis zu drei Stufen und ist **schriftlich zu dokumentieren**.

1. Zunächst müssen alle Verantwortlichen eine **systematische Risikobewertung (Schwellwertanalyse)** vornehmen, um zu prüfen, ob eine weitere Datenschutzfolgeabschätzung notwendig ist. Hier müssen einzelne Prozesse daraufhin überprüft werden, ob im Einzelfall voraussichtlich ein **hohes Risiko** für die Rechte und Freiheiten natürlicher Personen besteht. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlichem Risiko reicht eine gemeinsame Abschätzung (Art. 35 Abs. 1 S. 2 DSGVO).

Ein solches Risiko besteht nach Art. 35 Abs. 3 DSGVO insbesondere bei der Verwendung neuer Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten. Auch aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung kann ein solches Risiko bestehen. Schließlich kann die Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten oder Religionszugehörigkeit gemäß Art. 9 DSGVO) eine weitere Prüfung notwendig machen.

Doch auch wenn besonders schützenswerte Daten verarbeitet werden, bedeutet das nicht zwangsweise, dass auch ein hohes Risiko besteht – dies hängt vom bestehenden Sicherheitskonzept ab. Letztlich gibt es an diesem Punkt noch keine Rechtssicherheit.

Als Hilfestellung für die Einschätzung dienen die ersten „Leitlinien zu DSFA der Art.-29-Datenschutzgruppe“. Die Aufsichtsbehörden veröffentlichen darin gemäß Art. 35 Abs. 4 DSGVO eine Liste von Verarbeitungsvorgängen, für die eine Datenschutzfolgenabschätzung verbindlich durchzuführen ist (sogenannte „Blacklist“). Polen hat bereits solche Liste zusammengestellt, Belgien sogar zwei: eine Blacklist mit Verarbeitungstätigkeiten, die eine DSFA erforderlich machen, und eine sogenannte „Whitelist“, bei denen auf eben diese verzichtet werden kann.

2. Wenn ein Risiko im Hinblick auf den Prozess besteht, ist in einer 2. Stufe eine **Bewertung** vorzunehmen, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichen, um den **Schutz der Daten** zu gewährleisten. Außerdem ist nachzuweisen, dass die DSGVO eingehalten und die Interessen der Betroffenen berücksichtigt werden.

3. Kommt die Bewertung zu dem Ergebnis, dass trotz technischer und organisatorischer Maßnahmen ein hohes Risiko für die Rechte und Freiheiten der natürlichen Person verbleibt, muss die **Aufsichtsbehörde konsultiert werden** (Art. 36 Abs. 1 DSGVO). Diese kann dann innerhalb von acht Wochen Empfehlungen aussprechen (Art. 36 Abs. 2 DSGVO). Diese Frist kann je nach Komplexität der geplanten Verarbeitung von personenbezogenen Daten von der Aufsichtsbehörde verlängert werden.

Ist in dem Unternehmen ein Datenschutzbeauftragter bestellt, wird dieser auf Anfrage beratend in die Durchführung einer Datenschutz-Folgenabschätzung eingebunden (Art. 35 Abs. 2 und Art. 39 Abs. 1 c DSGVO).

11.8. Verzeichnis der Verarbeitungstätigkeiten erstellen?

Grundsätzlich ist jeder Verantwortliche und neuerdings auch jeder Auftragsverarbeiter verpflichtet, ein „Verzeichnis der Verarbeitungstätigkeiten“ (Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DSGVO bzw. Kategorieverzeichnis nach Art. 30 Abs. 2 DSGVO) zu führen und auf Verlangen der Aufsichtsbehörde zu Verfügung zu stellen, um dieser die Einhaltung der Vorschriften der DSGVO zu ermöglichen. Nach Art. 30 Abs. 5 DSGVO sind sowohl Verantwortliche als auch Auftragsverarbeiter von der Verzeichnispflicht ausgenommen, wenn sie weniger als 250 Mitarbeiter beschäftigen. Doch auch kleinere Unternehmen sind zum Führen eines Verarbeitungsverzeichnisses verpflichtet, wenn für sie nach Art. 30 Abs. 5 DSGVO gilt:

- Die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen. Wenn ein Verantwortlicher also nach Art. 35 Abs. 1 DSGVO verpflichtet ist, eine Datenschutz-Folgeabschätzung durchzuführen, muss er meist auch ein Verzeichnis der Verarbeitungstätigkeiten führen.
- Die Verarbeitung erfolgt nicht nur gelegentlich. Betroffen sind zum Beispiel alle Unternehmen, die regelmäßig Kundendaten speichern.

- Es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 DSGVO (z. B. Religions- oder Gesundheitsdaten) bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art 10 DSGVO.

Letztlich werden viele Unternehmen diese Voraussetzungen erfüllen. Doch ein solches Verzeichnis ist auch im Hinblick auf die gesamte datenschutzkonforme Umstellung sinnvoll, denn es gibt einen Überblick über alle Prozesse im Unternehmen und zeigt auf, was noch zu tun ist. Schließlich genügt das Unternehmen mit einem solchen Verzeichnis auch bereits einem Teil seine Rechenschaftspflicht (siehe unten).
Bei dem Verzeichnis der Verarbeitungstätigkeiten handelt es sich um eine Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden, ähnlich dem bisherigen Verfahrensverzeichnis des BDSG a. F. besteht bereits ein solches, kann dies als Grundlage herangezogen und aktualisiert werden.

Dazu werden zunächst **alle Geschäftsprozesse aufgelistet**, in denen personenbezogene Daten verarbeitet werden. Da in fast allen sowohl internen als auch externen Prozessen Daten verarbeitet werden, empfiehlt sich eine möglichst **feingliedrig Darstellung**, um die Geschäfte möglichst umfangreich abzubilden.

Anschließend müssen die in Art. 30 DSGVO genannten Angaben in das Verzeichnis mit aufgenommen werden. Zu identifizieren ist, woher die Daten in den jeweiligen Prozessen stammen, zu welchem Zweck sie verarbeitet werden, wer Zugriff hat und an wen sie weitergegeben werden. Zudem sind alle in Art. 30 Abs. 1 DSGVO genannten Punkte aufzulisten.

11.9. Der Rechenschaftspflicht nachkommen

Verantwortliche sind über das Führen eines Verzeichnisses der Verarbeitungstätigkeiten hinaus dafür zuständig, die **Einhaltung der Datenschutzgrundsätze** (Art. 5 Abs. 1 DSGVO: Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Verfügbarkeit, Integrität und Vertraulichkeit, Belastbarkeit, Intervenierbarkeit und Verarbeitung nach Treu und Glauben) gegenüber der Aufsichtsbehörde nachzuweisen (**Rechenschaftspflicht**, Art. 5 Abs. 2 DSGVO).

Damit sind nicht nur alle Datenverarbeitungstätigkeiten, sondern auch die Maßnahmen zur Einhaltung der Anforderungen der DSGVO zu dokumentieren. Mit dem Verzeichnis der Verarbeitungstätigkeiten ist schon ein Teil der Rechenschaftspflicht erfüllt. Hinzu kommt noch etwa die Dokumentation rechtmäßiger Einwilligungen, ein Nachweis, dass die personenbezogenen Daten rechtmäßig verarbeitet werden, oder das Ergebnis einer etwaigen Datenschutzfolgenabschätzung.

Auch diejenigen, die kein Verzeichnis der Verarbeitungstätigkeiten führen, müssen gegenüber der Aufsichtsbehörde nachweisen können, dass sie sich an die DSGVO halten.

Empfehlenswert ist es darüber hinaus, alle datenschutzrechtlich relevanten Maßnahmen in einer für das Unternehmen verbindlichen **Datenschutz- bzw. Informationssicherheitsleitlinie** zu dokumentieren. Dieses Dokument dient nicht nur dem Nachweis gegenüber der Aufsichtsbehörde, sondern auch zur eigenen Übersicht und zur Anleitung der Mitarbeiter. Darin sollten alle Aspekte

enthalten sein, die dazu dienen, die DSGVO intern konkret umzusetzen. Auch sollte klar geregelt sein, wer für welchen Bereich verantwortlich ist.

11.10. Einen Datenschutzbeauftragten bestellen?

Nach der DSGVO sind zunächst alle öffentlichen Stellen – mit Ausnahme von Gerichten – immer zur Bestellung eines Datenschutzbeauftragten verpflichtet. Verpflichtet sind außerdem Stellen, deren Kerntätigkeit

> *„in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen“,*

oder die Verarbeitung besonders sensibler personenbezogener Daten im Sinne der Art. 9 (z. B. Sexualität, Gesundheit, Religion) und 10 DSGVO ist.

Hier stellt sich die Frage, wann eine Verarbeitung auch die Kerntätigkeit eines Unternehmens ist. Bei vielen Branchen ist diese Auslegungsfrage noch nicht geklärt. Eine Redaktion dürfte aber nicht darunter fallen.

Allerdings macht auch das BDSG n. F. den – internen oder externen – Datenschutzbeauftragten dann zur Pflicht, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Datenverarbeitung beschäftigt sind (§ 38 Abs. 1 BDSG n. F.). Da in einem modernen Unternehmen, aber auch in einer Redaktion jeder Mitarbeiter ständig am Computer Daten verarbeitet, ist ein Datenschutzbeauftragter ab dieser Größe Pflicht.

Auch wenn die meisten nicht-öffentlichen Stellen damit nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, erlaubt eine Öffnungsklausel in der DSGVO den EU-Mitgliedsstaaten eigene, weitergehende Regelungen in diesem Bereich. In der neuen Fassung des BDSG hat der deutsche Gesetzgeber hiervon Gebrauch gemacht. Allerdings unterscheidet sich die neue Regelung im BDSG nicht wesentlich von der alten.

Für größere Unternehmen ist schließlich Art. 37 Abs. 2 DSGVO (entsprechender Verweis im BDSG n. F.) interessant, nach dem die Bestellung eines einzigen Datenschutzbeauftragten für mehrere Niederlassungen erlaubt ist (sogenannter „gemeinsamer“ oder „Konzerndatenschutzbeauftragter“). Voraussetzung ist zwar, dass der gemeinsame Datenschutzbeauftragte von jeder Niederlassung aus „leicht erreichbar“ ist, doch bezieht sich diese Anforderung nicht auf die körperliche Anwesenheit, sondern auf die Möglichkeit zum Austausch – etwa per Videokonferenz.

In jedem Fall muss ein Datenschutzbeauftragter beruflich und fachlich qualifiziert sein und sich regelmäßig fortbilden (Art. 37 Abs. 5 DSGVO). Die Benennung ist zu veröffentlichen und der Datenschutz-Aufsichtsbehörde zu melden (Art. 37 Abs. 7 DSGVO). Wird ein **interner** Datenschutzbeauftragter eingesetzt, gilt:

- Nach Art. 38 DSGVO ist der Datenschutzbeauftragte frühzeitig einzubinden, fachlich weisungsfrei und berichtet unmittelbar der höchsten Managementebene. Damit keine Interessenkonflikte entstehen, darf es sich nicht um ein Mitglied der Leitung des Unternehmens, einen IT- oder Personalverantwortlichen handeln. Ansonsten darf der Datenschutzbeauftragte aber durchaus auch andere Aufgaben im Unternehmen wahrnehmen, sofern Interessenkollisionen ausgeschlossen werden können (Art. 38 Abs. 6 S. 2 DSGVO).
- Zu berücksichtigen sind die Kosten für die Aus- und Fortbildung eines internen Datenschutzbeauftragten sowie der zeitliche Aufwand (Art. 38 Abs. 2 DSGVO). Entsprechende Ausbildungen bieten etwa Landessteuerberaterverbände oder die DATEV an. Auch ohne Pflicht zur Benennung sollte eine Person ausgebildet werden, die sich intern mit dem Thema Datenschutz auseinandersetzt (dies kann auch die Leitung des Unternehmens sein).
- Ein interner Datenschutzbeauftragter darf nach Bürgerlichem Gesetzbuch (§ 626 BGB) ohne wichtigen Grund weder abberufen noch gekündigt werden.

Übrigens: Auch wenn keine Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht, kann ein solcher als externe Hilfe zurate gezogen werden.

Hinweis: In Nordrhein-Westfalen können die Kontaktdaten eines Datenschutzbeauftragten erst ab dem 25. Mai mitgeteilt werden. Unterlassene Meldungen werden während einer Übergangszeit bis zum 31.12.2018 nicht als Datenschutzverstöße verfolgt oder geahndet werden.

Über die Autoren

Anne-Christine Herr leitet zusammen mit ihrem Kollegen die Presseabteilung der Kanzlei WILDE BEUGER SOLMECKE. Sie ist Volljuristin mit Schwerpunkt Medienrecht sowie Kunsthistorikerin. Vor ihrer jetzigen Tätigkeit hat sie u. a. als Redakteurin der Legal Tribune Online, einem juristischen Online-Magazin, gearbeitet.

Christian Solmecke hat sich als Rechtsanwalt und Partner der Kölner Medienrechtskanzlei WILDE BEUGER SOLMECKE auf die Beratung der Internet und IT-Branche spezialisiert. So hat er in den vergangenen Jahren den Bereich Internetrecht/E-Commerce der Kanzlei stetig ausgebaut und betreut zahlreiche Medienschaffende, Web 2.0 Plattformen und App-Entwickler.