PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Handbuch für Journalisten

Autoren: Iñigo de Miguel Beriain, Lorena Pérez Campillo (UPV/EHU)

Editor: Federico Caruso (OBC Transeuropa)

Inhaltsverzeichnis

1. Einleitung

Die Welt des Journalismus ist in Bezug auf den Datenschutz ein ganz besonderer Mikrokosmos. Obwohl er die Sammlung und Speicherung riesiger Mengen personenbezogener Daten in Form von Interviews, Unternehmensaufzeichnungen, Fotos und Filmen sowie deren Verbreitung beinhaltet, war der Rechtsrahmen noch nie vollkommen klar. Es ist daher nicht überraschend, dass es im Zusammenhang mit der Medientätigkeit ernsthafte Bedenken in Bezug auf den Datenschutz gibt (Erdos, 2015, S.8). In der Tat kann die Veröffentlichung von Informationen über eine identifizierte oder identifizierbare Person einen ernsthaften Angriff auf deren Privatsphäre darstellen.

Andererseits ist es unbestreitbar, dass die Arbeit des Journalismus für die Bildung einer gut informierten öffentlichen Meinung von wesentlicher Bedeutung ist. In der Tat werden die Mitglieder der Medien oft als öffentliche Wächter betrachtet, die in einer demokratischen Gesellschaft eine wichtige Rolle spielen. Sie haben die Pflicht, Informationen zu verbreiten und die Öffentlichkeit über alle Angelegenheiten von öffentlichem Interesse zu informieren, worauf die Öffentlichkeit auch ein Recht hat (Leitlinien zum Schutz der Privatsphäre in den Medien, S.6). Daher sind die Massenmedien verpflichtet, über Ereignisse, die von öffentlichem Interesse sein könnten, angemessen zu berichten, auch wenn dadurch die Rechte einiger Betroffener gefährdet werden können.

Es gibt also zwei Grundrechte, das Recht auf freie Meinungsäußerung und das Recht auf Privatsphäre, die manchmal miteinander kollidieren. Dies wirft ein Problem auf, das nur durch eine angemessene Abwägung in jedem konkreten Fall gelöst werden kann. Wann überwiegt das Recht auf den Schutz personenbezogener Daten gegenüber dem Recht auf freie Meinungsäußerung und Informationsfreiheit und umgekehrt? Diese Frage ist aus rechtlicher Sicht bereits eingehend erörtert worden. Die Verabschiedung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

(Datenschutz-Grundverordnung, DSGVO) und der verstärkte Schutz der Datenschutzrechte öffnen jedoch das Tor zu neuen Debatten. Wir glauben, dass Journalisten und Massenmedienorganisationen sich dieser Situation bewusst sein sollten.

Dieses Handbuch zielt nicht darauf ab, sich auf theoretische Aspekte dieses Themas zu konzentrieren, sondern Informationsfachleuten - Journalisten, Informationsredakteuren, Mediendirektoren usw. - geeignete Mechanismen an die Hand zu geben, um die Einhaltung der rechtlichen und ethischen Mindeststandards im Bereich des Datenschutzes zu gewährleisten und gleichzeitig eine angemessene Ausübung ihres Berufs sicherzustellen. Dieses Handbuch richtet sich an alle, die in einer Medienorganisation tätig sind, da sie alle von den Ausnahmen oder Abweichungen profitieren können, die sich aus Artikel 85 Absatz 2 der Datenschutz-Grundverordnung ergeben.

In diesem Handbuch werden verschiedene Rechtsrahmen miteinander kombiniert: einerseits die EU-Verordnung, vor allem die Datenschutz-Grundverordnung (DSGVO), und andererseits die Regelungen des Europarats durch die Europäische Menschenrechtskonvention und das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108). Diese Quellen werden durch die Rechtsprechung des EGMR und des EuGH ergänzt. Die Artikel-29-Datenschutzgruppe stellte fest: "Ein wichtiges Element, das sich aus der derzeitigen Rechtslage in den Mitgliedstaaten ergibt, ist, dass die Medien oder zumindest die Presse verpflichtet sind, bestimmte Vorschriften einzuhalten, die zwar nicht Teil der Datenschutzvorschriften im eigentlichen Sinne sind, aber zum Schutz der Privatsphäre des Einzelnen beitragen. Diese Rechtsvorschriften und die oft umfangreiche Rechtsprechung zu diesem Thema bieten spezifische Rechtsbehelfe, die manchmal als Ersatz für die fehlenden präventiven Rechtsbehelfe nach dem Datenschutzrecht angesehen werden" (A29WP, S. 7). Die in diesem Handbuch gegebenen Hinweise sollen sich daher an den von allen genannten Organen erlassenen Vorschriften orientieren.

Das Handbuch ist in mehrere Teile gegliedert. In den ersten Abschnitten wird der rechtliche Rahmen für Journalismus und Datenschutzfragen in der EU erläutert. Die

Abschnitte vier und fünf befassen sich stattdessen mit den wichtigsten ethischen Fragen, die ein Journalist oder eine Medienorganisation im Rahmen der Datenschutz-Grundverordnung und der Verordnungen des Europarats zu behandeln hat. Die Anhänge schließlich enthalten detaillierte Informationen über die Abwägungsprüfung und den Rechtsrahmen auf der Ebene der Mitgliedstaaten.

DISCLAIMER: Dieses Dokument soll Journalisten im Umgang mit der Datenschutzverordnung unterstützen. Sein Inhalt stellt jedoch keine Rechtsberatung dar, ist nicht als Ersatz für eine Rechtsberatung gedacht und sollte nicht als solcher verwendet werden. Sie sollten sich in Bezug auf bestimmte Angelegenheiten, die Sie oder Ihre Organisation betreffen, rechtlich oder anderweitig professionell beraten lassen.

2. Der Rechtsrahmen für Meinungsfreiheit und Datenschutz in der EU-Arena

Der Rechtsrahmen für das Recht auf freie Meinungsäußerung und den Datenschutz in Europa ist hauptsächlich mit den Rechtssystemen des Europarats und der Europäischen Union verbunden. Im Falle des Europarats ist die Regelung zweigeteilt. Einerseits sind die wichtigsten Rechte, um die es geht, das Recht auf freie Meinungsäußerung und das Recht auf Privatsphäre, Teil der Europäischen Menschenrechtskonvention. In Artikel 10.1 heißt es: "Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht umfasst die Freiheit der Meinungsäußerung sowie die Freiheit, Informationen und Gedankengut ohne behördliche Eingriffe und ohne Rücksicht auf Grenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht daran, die Erteilung von Lizenzen für Rundfunk-, Fernseh- oder Kinounternehmen zu verlangen. Es liegt auf der Hand, dass dieses Recht gemäß den Bestimmungen von Nummer 2 dieser Klausel eingeschränkt werden kann. Artikel 8 konzentriert sich stattdessen auf den Schutz der Privatsphäre, indem er festlegt, dass:

> "(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
>
> (2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft

> notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer."

Andererseits regelt das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108), das ebenfalls vom Europarat angenommen wurde, Fragen des Datenschutzes. Es ist gegenwärtig das einzige rechtsverbindliche internationale Abkommen zum Datenschutzrecht. Der Europäische Gerichtshof für Menschenrechte befasst sich jedoch nicht mit Fällen, in denen es um angebliche Verstöße gegen dieses Übereinkommen geht, da es sich nur auf die Europäische Menschenrechtskonvention bezieht.

Im EU-Kontext wurde das Recht auf freie Meinungsäußerung in Artikel 11 der EU-Grundrechtecharta aufgenommen, der wie folgt lautet

> "(1) Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben.
>
> (2) Die Freiheit der Medien und ihre Pluralität werden geachtet".

Stattdessen enthalten die Artikel 7 und 8 der Charta das Recht auf Privatsphäre und das Recht auf den Schutz der sie betreffenden personenbezogenen Daten. Gegenwärtig wird der rechtliche Rahmen für den Datenschutz hauptsächlich durch die Verordnung (EU) 2016/679 der Datenschutz-Grundverordnung (DSGVO) abgesteckt. Angebliche Verstöße gegen das EU-Recht werden vor dem Gerichtshof der Europäischen Union (EuGH) verhandelt. Es gibt keine gleichwertigen übergreifenden und umfassenden sekundären Rechtsvorschriften über die freie Meinungsäußerung und die Medienfreiheit, was hauptsächlich auf den Standpunkt der Kommission zurückzuführen ist, dass die EU nicht befugt ist, in diesem Bereich Rechtsvorschriften zu erlassen (Biriukova, 6).

Die Datenschutz-Grundverordnung gilt immer dann, wenn jemand Informationen über eine lebende Person verarbeitet (z. B. sammelt, aufbewahrt, nutzt oder weitergibt). Wie das Information Commissioner's Office (ICO) anmerkt, "steht sie verantwortungsvollem Journalismus nicht im Wege, da die wichtigsten Grundsätze flexibel genug sind, um alltäglichen journalistischen Praktiken Rechnung zu tragen (...) Die Medien sind jedoch nicht automatisch ausgenommen und müssen sicherstellen, dass sie die Datenschutzrechte von Einzelpersonen berücksichtigen. Die rechtliche Verantwortung liegt in der Regel bei der jeweiligen Medienorganisation und nicht bei den einzelnen Mitarbeitern, obwohl freiberufliche Journalisten wahrscheinlich eigene Verpflichtungen haben". Es ist jedoch ratsam, sich immer vor Augen zu halten, dass die Mitarbeiter von Medienorganisationen sich ihrer rechtlichen Verantwortung bewusst sein müssen, insbesondere was die tägliche Einhaltung betrifft, wenn sie für ihren Arbeitgeber arbeiten.

3. Die "journalistische Ausnahme" in der GDPR

3.1 Einleitung und Hintergrund

Die Datenschutz-Grundverordnung ist das wichtigste Rechtsinstrument für Datenschutzfragen auf EU-Ebene. Sie enthält die allgemeinen Grundsätze und Regeln, die für jede Verarbeitung personenbezogener Daten innerhalb der EU oder von EU-Bürgern gelten. In ihren Bestimmungen ist es möglich, einen spezifischen Hinweis auf die fraglichen Fragen zu finden. Es handelt sich um die so genannte "journalistische Ausnahmeregelung" gemäß Artikel 85 der Datenschutz-Grundverordnung, die in der nachstehenden Tabelle aufgeführt ist.

Diese Klausel wurde in die Datenschutz-Grundverordnung aufgenommen, um die Spannungen zwischen dem Recht auf freie Meinungsäußerung und dem Recht auf Datenschutz abzumildern. In der Tat sollte damit die allgemeine Notwendigkeit kodifiziert werden, ein Gleichgewicht zwischen diesen beiden Grundrechten herzustellen. Auf den ersten Blick wurde den Mitgliedstaaten lediglich die Möglichkeit eingeräumt, diejenigen, die ihr Recht auf freie Meinungsäußerung zu "journalistischen Zwecken" ausüben, von bestimmten Vorschriften und Verpflichtungen der DSGVO auszunehmen (Biriukova, 14).

Diese Ausnahmeregelung für Journalisten war kein Novum in der EU-Verordnung. Artikel 9 der Datenschutzrichtlinie von 1995, dem Vorläufer der Datenschutz-Grundverordnung, enthielt bereits eine ähnliche Bestimmung, was zu einer gewissen Divergenz bei der Regelung dieser Frage in den EU-Mitgliedstaaten führte. In einer Empfehlung der Artikel-29-Datenschutzgruppe wurde die Situation [1]zusammengefasst, indem die Mitgliedstaaten in drei Hauptgruppen unterteilt wurden:

> "a) In einigen Fällen enthalten die Datenschutzvorschriften keine ausdrückliche Ausnahme von der Anwendung ihrer Bestimmungen auf die Medien. Dies ist derzeit in Belgien, Spanien, Portugal, Schweden und dem Vereinigten Königreich der Fall.
>
> b) In anderen Fällen sind die Medien von der Anwendung mehrerer Datenschutzbestimmungen ausgenommen. Dies ist derzeit in Deutschland, Frankreich, den Niederlanden, Österreich und Finnland der Fall. Ähnliche Ausnahmeregelungen sind im italienischen Gesetzesentwurf vorgesehen.
>
> c) In anderen Fällen sind die Medien von den allgemeinen Datenschutzgesetzen ausgenommen und werden durch spezifische Datenschutzbestimmungen geregelt. Dies gilt in Dänemark für alle Medien und in Deutschland für die öffentlich-rechtlichen Rundfunkanstalten, die nicht unter die Datenschutzgesetze des Bundes oder der Länder fallen, sondern besonderen Datenschutzbestimmungen in den für sie geltenden Staatsverträgen unterliegen".

Die Datenschutz-Grundverordnung hat an diesem Szenario nur geringfügige Änderungen vorgenommen. Tatsächlich bietet Artikel 85 der DSGVO den Mitgliedstaaten einen sehr breiten Handlungsrahmen. Sie sollen den Umfang der journalistischen Ausnahmeregelung und die Umstände, unter denen sie gilt, festlegen. Damit ihre regulatorischen Entwicklungen gültig sind, müssen sie jedoch mit den

1 Die Datenschutzgruppe stellte jedoch auch fest: "Die Unterschiede zwischen diesen drei Modellen sollten jedoch nicht überbewertet werden. In den meisten Fällen gelten die Datenschutzvorschriften - unabhängig von etwaigen ausdrücklichen Ausnahmeregelungen - aufgrund des besonderen verfassungsrechtlichen Status der Vorschriften über die Meinungs- und Pressefreiheit nicht uneingeschränkt für die Medien. Diese Vorschriften schränken die Anwendung der materiellen Datenschutzbestimmungen oder zumindest ihre wirksame Durchsetzung de facto ein. Auf der anderen Seite die gewöhnlichen Daten". Siehe: Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten, Datenschutzrecht und Medien, Empfehlung 1/97, S. 6-7, unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf.

Bestimmungen der Datenschutz-Grundverordnung und der Europäischen Menschenrechtskonvention (EMRK) in Einklang gebracht werden. Daher muss man die Regeln, die im journalistischen Umfeld zu befolgen sind, aus einer doppelten Perspektive betrachten. Einerseits muss man immer eine Reihe von Regeln im Auge behalten, die in der DSGVO und/oder der EMRK sowie in der Rechtsprechung des EuGH und des EGMR verankert sind. Diese müssen bei der Ausübung dieses Berufs strikt befolgt werden. Andererseits ist zu berücksichtigen, dass es je nach dem jeweiligen Rechtsrahmen gewisse Unterschiede zwischen den Mitgliedstaaten geben kann. In jedem Fall sollten sie nicht übermäßig groß sein, da die Grundsätze und Regeln der Datenschutz-Grundverordnung und der EMRK immer eingehalten werden müssen.

Dennoch ist es wichtig, darauf hinzuweisen, dass sich einige Mitgliedstaaten nicht vollständig an diese Standards gehalten haben. In Bulgarien zum Beispiel hat das Verfassungsgericht kürzlich den nationalen Ansatz zur Umsetzung von Artikel 85 für verfassungswidrig erklärt. Grund dafür war die Aufnahme eines Artikels in das Gesetz zum Schutz personenbezogener Daten, in dem zehn Kriterien festgelegt sind, anhand derer entschieden wird, ob Journalisten das Gleichgewicht zwischen dem Recht auf Information und dem Recht auf Schutz personenbezogener Daten eingehalten haben. Das Gericht vertrat die Auffassung, dass diese Kriterien zu vage seien und die Gefahr willkürlicher Auslegungen bergen könnten, ein Umstand, der der Datenschutzkommission eine unvorhersehbare Auslegungsbefugnis eröffnete, die nicht unbedingt dem öffentlichen Interesse an einer pluralistischen Information über die Politik und die Aktivitäten der Regierung entspricht[2].

Darüber hinaus wurde die rumänische Datenschutzbehörde dafür kritisiert, dass sie die Datenschutz-Grundverordnung nutzt, um kritische Stimmen in den nationalen Medien zum Schweigen zu bringen. Im November 2018 wurde in Rumänien über einen Fall berichtet, der das Spannungsverhältnis zwischen Datenschutz und Meinungsfreiheit gut widerspiegeln könnte. Er stand im Zusammenhang mit einem Artikel über einen Korruptionsskandal, in den ein Politiker und seine engen Beziehungen zu einem Unternehmen, gegen das wegen Betrugs ermittelt wird, verwickelt waren und der auf

2 Bulgariens Verfassungsgericht lehnt Datenschutzklausel ab, 17. November 2019, https://sofiaglobe.com/2019/11/17/bulgarias-constitutional-court-rejects-data-protection-law-clause-on-media/#:~:text=Bulgariens%20Verfassungsgericht%20hat%20geurteilt,dass%20der%20persönliche%20Datenschutz%20ist.

der Facebook-Seite des in Bukarest ansässigen Rise Project veröffentlicht wurde. Einige Zeit nach der Veröffentlichung schickte die rumänische Datenschutzbehörde (ANSPDCP) eine Reihe von Fragen an die Journalisten, die den Artikel verfasst hatten.

Theoretisch war dies auf die Notwendigkeit zurückzuführen, ein Gleichgewicht zwischen dem Recht auf den Schutz personenbezogener Daten, der freien Meinungsäußerung und dem Recht auf Information zu gewährleisten. Die Behörde war der Ansicht, dass die Journalisten von Rise gegen die Datenschutz-Grundverordnung verstoßen hatten, indem sie die Videos, Fotos und Dokumente - im Wesentlichen die privaten Daten rumänischer Bürger - veröffentlichten, um die Behauptungen der Reporter zu untermauern. Die Journalisten wurden um Informationen gebeten, die die Quellen des Artikels offenlegen könnten, unter dem Hinweis, dass sie mit einer Strafe von bis zu 20 Millionen Euro rechnen müssten, wenn sie nicht kooperieren würden (Warner, 2019).

Eine Gruppe von zwölf Menschenrechts- und Medienorganisationen reagierte auf diese Aufforderung mit einem offenen Brief an die ANSPDCP, in dem sie die ANSPDCP aufforderte, Fälle, die das Recht auf freie Meinungsäußerung gefährden könnten, sorgfältig zu analysieren. Sie forderten außerdem die Einrichtung eines dringenden und transparenten Mechanismus zur Beurteilung von Klagen, die Datenverarbeitungsvorgänge zu journalistischen Zwecken betreffen. Zur gleichen Zeit schickten sechzehn NRO für digitale Rechte ein Schreiben an den Europäischen Datenschutzausschuss, mit einer Kopie der ANSPDCP und der Europäischen Kommission, in dem sie forderten, dass die DSGVO nicht missbraucht werden dürfe, um die Medienfreiheit in Rumänien zu gefährden (Benezic, 2018). Später kritisierten einige Abgeordnete des Europäischen Parlaments in Brüssel das Verfahren gegen das Rise Project und bestritten die rumänische Auslegung der Durchsetzung der DSGVO. All dies führte schließlich zu Warnungen seitens der Europäischen Kommission (Nielsen, 2018). Zum jetzigen Zeitpunkt ist es jedoch schwer zu sagen, was letztendlich passieren wird, da der Fall noch nicht abgeschlossen ist.

Es gibt jedoch einige andere Mitgliedstaaten, die den entgegengesetzten Weg eingeschlagen haben. Schweden vertrat beispielsweise die Auffassung, dass Artikel 85 der Datenschutz-Grundverordnung den Mitgliedstaaten einen größeren Spielraum für

Ausnahmen einräumt als die Datenschutzrichtlinie, nicht zuletzt deshalb, weil er nicht verlangt, dass die Verarbeitung "ausschließlich" zu journalistischen Zwecken erfolgen muss (eine Formulierung, die in der Richtlinie enthalten war). Darüber hinaus machte die schwedische Regierung geltend, dass Erwägungsgrund 153 der Datenschutz-Grundverordnung besagt, dass das Konzept der freien Meinungsäußerung weit auszulegen ist. Auf dieser Grundlage enthält das neue Datenschutzgesetz umfassendere Ausnahmen oder Abweichungen als das Gesetz über personenbezogene Daten von 1998 (McCullagh, 45).

3.2 Der persönliche Geltungsbereich der Freistellung

Was bedeutet "journalistische Zwecke"? Was bedeutet "Journalismus"? In der Verordnung gibt es keine Definition des Begriffs "Journalismus", da er aus den ersten Entwürfen der Datenschutz-Grundverordnung[3] gestrichen wurde. Einige Mitgliedstaaten haben ihre eigenen Definitionen erstellt. Die meisten von ihnen sind recht offen, mit der großen Ausnahme Österreichs, das die Ausnahmeregelung ausschließlich "Medienunternehmen, Mediendiensten und deren Beschäftigten" vorbehält (Cullagh, 2019, S.5).

Es scheint jedoch ziemlich klar zu sein, dass die Datenschutz-Grundverordnung sich für eine offene, umfassende Bedeutung des Begriffs entscheidet, die anwendbar sein könnte, auch wenn die nationale Regelung dies nicht widerspiegelt. In der Rechtssache[4] Buivids akzeptierte der EuGH, dass die Ausnahmeregelung für Journalisten auf einen Bürger anwendbar ist, der eine Videoaufzeichnung auf Youtube veröffentlichte und nachwies, dass der Zweck der Aufzeichnung und Veröffentlichung die Weitergabe von Informationen, Meinungen oder Ideen an die Öffentlichkeit war. In ähnlicher Weise entschied der EuGH in der Rechtssache[5] Satamedia, dass die Erhebung und Verbreitung von Daten ebenfalls als "journalistisch" angesehen werden kann, wenn sie unabhängig

3 In der Tat lautete der Entwurf: "Die Mitgliedstaaten sollten Tätigkeiten als "journalistisch" im Sinne der in dieser Verordnung festzulegenden Ausnahmen und Befreiungen einstufen, wenn diese Tätigkeiten die Weitergabe von Informationen, Meinungen oder Gedankengut an die Öffentlichkeit zum Gegenstand haben, unabhängig davon, welches Medium zu ihrer Übermittlung verwendet wird. Sie sollten nicht auf Medienunternehmen beschränkt sein und können mit oder ohne Gewinnerzielungsabsicht ausgeübt werden" (Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM/2012/011, https://eur-lex.europa.eu/ legal-content/EN/TXT/?uri=CELEX%3A52012PC0011).

4 EuGH, Sergejs Buivids v. Datu valsts inspekcija, C-345/17, 14. Februar 2019.

5 EuGH, Tietosuojavaltuutettu gegen Satakunnan Markkinapörssi Oy und Satamedia Oy, C-73/07, 16. Dezember 2008

von den verwendeten Mitteln darauf abzielt, Informationen, Meinungen oder Ideen an die Öffentlichkeit weiterzugeben. Die Tatsache, dass es sich bei dem für die Verarbeitung Verantwortlichen um eine nicht auf Gewinn ausgerichtete Medienorganisation handelt, wurde als irrelevant für diese Zwecke angesehen.

Es ist nicht klar, was passieren würde, wenn eine österreichische Organisation, die als Medienunternehmen oder Mediendienst angesehen werden könnte, eine der in Artikel 85 vorgesehenen Abweichungen oder Ausnahmen anwendet. In gewisser Weise würde dies zu einem Konflikt zwischen der österreichischen Verordnung und der Datenschutz-Grundverordnung führen, die ausdrücklich eine breite Ausweitung des Begriffs "Journalismus" vorsieht. Unserer Meinung nach ist es wahrscheinlich, dass die Auslegung der Datenschutz-Grundverordnung Vorrang haben wird.

Vor diesem Hintergrund scheint eine weit gefasste Definition des Begriffs "Journalismus" viel sinnvoller zu sein als eine enge. Natalija Bitiukova hat geschrieben, dass "Journalismus sich auf die Produktion und Verbreitung von Informationen und Nachrichten an eine unbestimmte Anzahl von Menschen in Verfolgung des öffentlichen Interesses und als Beitrag zur öffentlichen Debatte bezieht" (Bitiukova, S.4). Ihre Formulierung passt unserer Meinung nach sehr gut zur DSGVO.

Journalismus muss daher als eine Tätigkeit definiert werden, die alle Ausgaben für Nachrichten, aktuelle Themen, Verbraucherfragen oder Sport[6] umfasst. Denn die Ausnahmeregelung gilt nur für Informationen, die für journalistische Zwecke verarbeitet werden. Der Begriff kann auch Herausgeber und Redakteure von Internet-Blogs oder Webseiten einschließen, da Kommentare auf diesen Plattformen als Ausdruck ihrer eigenen Meinungsfreiheit angesehen werden sollten. Dies bedeutet natürlich nicht, dass jeder Blog oder jeder Kommentar, der online gepostet wird, Journalismus ist, da einige Blogger einfach nur die Absicht haben, an allgemeinen sozialen Interaktionen oder anderen Freizeitaktivitäten im Internet teilzunehmen.

6 Das ICO erklärt: "Zusammen mit Kunst und Literatur umfasst der Begriff wahrscheinlich alles, was in einer Zeitung oder Zeitschrift veröffentlicht oder im Radio oder Fernsehen ausgestrahlt wird - mit anderen Worten, die gesamte Produktion der Print- und Rundfunkmedien, mit Ausnahme der bezahlten Werbung (...Kurz gesagt, die Ausnahmeregelung kann potenziell fast alle Informationen abdecken, die als Teil des täglichen Outputs der Presse- und Rundfunkmedien und vergleichbarer Online-Nachrichten- oder Nachrichtenkanäle gesammelt oder erstellt werdenIt would . a wide range of, into („ and Werbeeinnahmen, Vermögensverwaltung, Finanzschulden, Auflagenhöhe oder Öffentlichkeitsarbeit werden jedoch in der Regel nicht als Journalismus angesehen" (ICO, 29).

Außerdem sind Suchmaschinen ausdrücklich von dem Konzept und damit von der Ausnahme[7] ausgeschlossen.

3.3 Verarbeitung personenbezogener Daten: der sachliche Anwendungsbereich

Wie gezeigt, legt Artikel 85 fest, dass Ausnahmen oder Abweichungen für jeden gelten können, der Informationen, Meinungen oder Ideen an die Öffentlichkeit weitergeben will. Welche Art von Daten könnte jedoch als solche angesehen werden? Welche personenbezogenen Daten können zu journalistischen Zwecken verarbeitet werden, ohne dass die Datenschutz-Grundverordnung eingehalten werden muss? Auch auf diese Frage gibt es keine einfache Antwort. Grundsätzlich haben die Mitgliedstaaten ein Mitspracherecht bei der Festlegung des materiellen Anwendungsbereichs der Ausnahmeregelung für Journalisten, und ihre Politik ist nicht immer einheitlich. So bietet beispielsweise Artikel 7 des rumänischen Gesetzes Nr. 190/2018, das Ausnahmen für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken einführt, nur drei alternative Szenarien, unter denen personenbezogene Daten zu journalistischen Zwecken verarbeitet werden können[8]:

> 1) wenn es sich um personenbezogene Daten handelt, die von der betroffenen Person eindeutig öffentlich gemacht wurden;
>
> 2) wenn die personenbezogenen Daten in engem Zusammenhang mit der Eigenschaft der betroffenen Person als öffentliche Person stehen; oder
>
> 3) wenn die personenbezogenen Daten in engem Zusammenhang mit dem öffentlichen Charakter der Handlungen stehen, an denen die betroffene Person beteiligt ist. Wenn eine dieser drei Situationen zutrifft, ist die DSGVO (mit Ausnahme des Kapitels über Sanktionen) vollständig von der Anwendung ausgeschlossen.

7 EuGH, Google SL Spainund Google Inc. gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, C-131/12, 13 May 2014, par. 81

8 Beschwerde der Association for Technology and Internet (ApTI) an die EU-Kommission, 2018, unter: https://www.apti.ro/sites/default/files/Complaint%20on%20Romanian%20implementation%20of%20the%20GDPR%20-%20ApTI.pdf

Diese drei alternativen Szenarien sind im Vergleich zur aktuellen Rechtsprechung sowohl des Europäischen Gerichtshofs als auch des Europäischen Gerichtshofs für Menschenrechte äußerst begrenzt. Beide Gerichte sind der Ansicht, dass vor einer Analyse mehrere Faktoren abgewogen werden müssen, wobei die wichtigsten der Beitrag zu einer Debatte von öffentlichem Interesse einerseits und die Beeinträchtigung des Privatlebens der betroffenen Personen andererseits sind. Daher scheint das rumänische Recht keinen angemessenen Ausgleich zwischen dem Recht auf den Schutz personenbezogener Daten und dem Recht auf freie Meinungsäußerung und Informationsfreiheit zu schaffen.

Das Vereinigte Königreich hat einen völlig anderen Ansatz gewählt. In seinem Datenschutzgesetz 2018 wird die Auffassung vertreten, dass die Journalistenausnahme für die Verarbeitung personenbezogener Daten gilt, wenn drei kumulative Bedingungen erfüllt sind:

- die betreffenden Daten müssen im Hinblick auf die Veröffentlichung von journalistischem Material verarbeitet werden,
- der für die Verarbeitung Verantwortliche muss vernünftigerweise davon ausgehen, dass die Veröffentlichung unter besonderer Berücksichtigung der besonderen Bedeutung des öffentlichen Interesses an der freien Meinungsäußerung im öffentlichen Interesse liegt,
- und der für die Datenverarbeitung Verantwortliche muss vernünftigerweise davon ausgehen, dass die Anwendung der aufgeführten DSGVO-Bestimmung mit seinem journalistischen Zweck unvereinbar wäre.

Dieser Ansatz scheint viel besser mit dem Rechtsrahmen übereinzustimmen.

3.4. Die Bedingung für die Freistellung

Die in Artikel 85 vorgesehenen Ausnahmen oder Abweichungen sind nur anwendbar, "wenn sie erforderlich sind, um das Recht auf den Schutz personenbezogener Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen". Wann ist diese Notwendigkeit gegeben? Erwägungsgrund 153 gibt wertvolle Hinweise zur Beantwortung dieser Frage:

> *Im Recht der Mitgliedstaaten sollten die Vorschriften über die freie Meinungsäußerung und Informationsfreiheit, auch von Journalisten, Wissenschaftlern, Künstlern und/oder Schriftstellern, mit dem Recht auf Schutz der*

personenbezogenen Daten gemäß dieser Verordnung in Einklang gebracht werden. Für die Verarbeitung personenbezogener Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken sollten Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung gelten, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit dem Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit, wie es in Artikel 11 der Charta garantiert ist, in Einklang zu bringen. Dies sollte insbesondere für die Verarbeitung personenbezogener Daten im audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven gelten. Die Mitgliedstaaten sollten daher Gesetzgebungsmaßnahmen zur Regelung der Abweichungen und Ausnahmen erlassen, die zum Zwecke der Abwägung zwischen diesen Grundrechten notwendig sind.

Die Datenschutz-Grundverordnung ist also gewillt, ein angemessenes Gleichgewicht zwischen dem Datenschutz und dem Recht auf freie Meinungsäußerung und Information, wie es in Artikel 11 der Charta[9] verankert ist, zu gewährleisten. Aus diesem Grund gelten *Ausnahmen oder Befreiungen von bestimmten Bestimmungen der DSGVO* nur *dann, wenn dies erforderlich ist, um das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang zu bringen*. Dieser Gedanke der Abwägung zwischen beiden Rechten wurde durch die Rechtsprechung des EGMR und des EuGH bestätigt, wonach eine Abwägung von Fall zu Fall vorgenommen werden muss, wenn ein echter Konflikt zwischen diesen Rechten besteht. Der entscheidende Punkt ist jedoch, wie man dabei vorgeht. Das ICO erklärt, dass Organisationen dies in angemessener Weise tun können, indem sie Folgendes berücksichtigen

- das allgemeine öffentliche Interesse an der freien Meinungsäußerung,
- ein besonderes öffentliches Interesse an diesem Thema,
- das Ausmaß des Eingriffs in das Privatleben einer Person, einschließlich der Frage, ob die Geschichte auf eine weniger einschneidende Weise weiterverfolgt und veröffentlicht werden könnte, und
- der potenzielle Schaden, der Einzelpersonen zugefügt werden könnte. Bestehende Leitlinien, die in Verhaltenskodizes der Industrie niedergelegt sind,

9 Artikel 11. Freiheit der Meinungsäußerung und Informationsfreiheit

1. Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit ein, Meinungen zu vertreten sowie Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Grenzen zu empfangen und weiterzugeben.

2. Die Freiheit und der Pluralismus der Medien werden geachtet.

können Organisationen dabei helfen, darüber nachzudenken, was im öffentlichen Interesse[10] ist.

In diesem Zusammenhang ist der Begriff des öffentlichen Interesses nach der Rechtsprechung des Gerichtshofs der EU oder des Europäischen Gerichtshofs für Menschenrechte besonders relevant, wie in Fällen wie Buivids[11] oder Satakunnan gegen Finnland[12] erwähnt. Es ist jedoch schwer zu definieren. Tatsächlich hat der EGMR in der Vergangenheit davon abgesehen, eine Definition des Begriffs "öffentliches Interesse" zu geben. Dennoch erklärte er im Zusammenhang mit den Von-Hannover-Fällen[13], dass "ein erstes wesentliches Kriterium der Beitrag ist, den Fotos oder Presseartikel zu einer Debatte von allgemeinem Interesse leisten. Es scheint also, dass dieser Begriff "die öffentliche, politische und historische Debatte, Fragen im Zusammenhang mit Politikern, dem Verhalten von Staatsbediensteten, großen Unternehmen, Regierungen und kriminellen Angelegenheiten" umfasst. Aber auch andere, weniger offensichtliche Themen können als von öffentlichem oder allgemeinem Interesse angesehen werden" (Biriukova, 21).

Zusammenfassend lässt sich sagen, dass es einige Variablen gibt, die in der Definition des öffentlichen Interesses sicher vorhanden sein müssen, die "ein Element der Verhältnismäßigkeit beinhalten müssen - es kann nicht im öffentlichen Interesse sein, unverhältnismäßig oder unüberlegt in die grundlegenden Rechte einer Person auf Privatsphäre und Datenschutz einzugreifen. Wenn die Untersuchungsmethode oder die zu veröffentlichenden Details besonders einschneidend oder schädlich für eine Person sind, ist ein stärkeres und fallspezifisches Argument des öffentlichen Interesses erforderlich, um dies über das allgemeine öffentliche Interesse an der freien Meinungsäußerung hinaus zu rechtfertigen" (ICO, 33). In der Tat kann das öffentliche Interesse nicht auf den Informationsdurst der Öffentlichkeit über das Privatleben anderer oder auf den Wunsch des Lesers nach Sensationslust oder gar Voyeurismus reduziert werden, wie z. B. die Veröffentlichung von Einzelheiten über die sexuellen Aktivitäten einer Person des öffentlichen Lebens. Wenn das einzige Ziel eines Artikels darin besteht, die Neugier der Leserschaft auf Details aus dem Privatleben einer Person

10 ICO, S. 34

11 EuGH, Sergejs Buivids v. Datu valsts inspekcija, C-345/17, 14. Februar 2019, Rn. 60-61.

12 EGMR, Satakunnan Markkinapörssi Oy und Satamedia Oy gegen Finnland, App no 931/13, 21. Juli 2015.

13 EGMR, Von Hannover gegen Deutschland (Nr. 2), App Nos. 40660/08 und 60641/08, 7. Februar 2012, par. 109.

zu befriedigen, kann nicht davon ausgegangen werden, dass er zu einer Debatte von allgemeinem Interesse für die Gesellschaft beiträgt (Leitlinien für den Schutz der Privatsphäre in den Medien, 12). So wurde beispielsweise in der Rechtssache Standard Verlags GmbH gegen Österreich (Nr. 2) entschieden, dass eine Zeitung die Privatsphäre der Betroffenen verletzt hatte, als sie einen Artikel veröffentlichte, in dem sie Gerüchte kommentierte, wonach die Ehefrau des damaligen österreichischen Bundespräsidenten sich von ihm scheiden lassen wollte und enge Kontakte zu einem anderen Politiker unterhielt. Nach Ansicht des Gerichts dürfen Journalisten nicht über sinnlosen Klatsch und Tratsch über die Ehen von Politikern berichten. In den Leitlinien für den Schutz der Privatsphäre in den Medien wird hervorgehoben, dass es für Journalisten bei der Beurteilung, ob es sich bei einer Person des öffentlichen Lebens um eine Person des öffentlichen Lebens handelt, von geringer Bedeutung ist, ob eine bestimmte Person der Öffentlichkeit tatsächlich bekannt ist. Journalisten können sich nicht durch die Behauptung der betroffenen Personen einschränken lassen, sie seien der Öffentlichkeit nicht bekannt. Es kommt darauf an, ob die Person in die Öffentlichkeit getreten ist, indem sie an einer öffentlichen Debatte teilgenommen hat oder in einem Bereich von öffentlichem Interesse oder in der öffentlichen Debatte aktiv war" (Leitlinien zum Schutz der Privatsphäre in den Medien, 12-20). Eine Reihe von Beispielen für Sätze, die vom EGMR erstellt und in den Leitlinien zusammengestellt wurden, sind in die nächste Tabelle aufgenommen worden (die vollständigen Referenzen sind im Abschnitt Informationsquellen am Ende dieses Handbuchs enthalten).

Diese Überlegungen öffnen das Tor zu einer umfassenderen Debatte darüber, wie das öffentliche Interesse gegen das Recht auf Privatsphäre abgewogen werden kann. Dies wird in dem Abschnitt dieses Handbuchs analysiert, der dem berechtigten Interesse als Rechtsgrundlage für die Verarbeitung personenbezogener Daten gewidmet ist.

3.5 Der materielle Anwendungsbereich der Ausnahme

Artikel 85 legt einen breiten Anwendungsbereich für die Ausnahmen und Abweichungen fest, da er Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (für die Verarbeitung Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen), Kapitel VI (unabhängige Kontrollstellen), Kapitel VII (Zusammenarbeit

und Kohärenz) und Kapitel IX (besondere Datenverarbeitungssituationen) erwähnt. Ausnahmen und Abweichungen können sich daher auf die *allgemeinen Grundsätze, die Rechte der betroffenen Person, des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters, die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, die unabhängigen Kontrollstellen, die Zusammenarbeit und Kohärenz sowie auf besondere Datenverarbeitungssituationen beziehen.*

Es ist jedoch wichtig zu beachten, dass dieser breite Anwendungsbereich nicht unbedingt für alle EU-Mitgliedstaaten gilt. In der Klausel heißt es ausdrücklich, dass die Mitgliedstaaten Ausnahmen oder Abweichungen vorsehen sollen, doch werden diese Ausnahmen nicht aufgeführt. Sie erklärt lediglich, dass sie per Gesetz das Recht auf den Schutz personenbezogener Daten gemäß dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu Zwecken des wissenschaftlichen, künstlerischen oder literarischen Ausdrucks, miteinander in Einklang bringen *müssen*.

Die Entscheidung über die zu ergreifenden konkreten Maßnahmen liegt daher bei den Mitgliedsstaaten. Sie sollen einen solchen Rechtsrahmen entwickeln und der Kommission die angenommenen Bestimmungen über Ausnahmen oder Abweichungen sowie alle nachfolgenden Änderungsgesetze oder Änderungen, die sie betreffen, unverzüglich mitteilen. Zum jetzigen Zeitpunkt (November 2020) haben noch nicht alle Mitgliedstaaten einen solchen Rechtsrahmen entwickelt. In Anhang II haben wir Informationen über die von den EU-Mitgliedsstaaten übernommene Regelung aufgenommen, einschließlich der Daten, in denen die Änderung eingeführt wurde. Es kann jedoch vorkommen, dass einige Länder ihren Rechtsrahmen nachträglich geändert haben.

3.6 Anwendbare Verordnung

Im Allgemeinen sollten Journalisten versuchen, die Übermittlung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums (EWR) ohne angemessenen Schutz zu vermeiden. Was als "angemessener Schutz" gilt, hängt "unter anderem von der Art der Informationen, dem Zweck der Übermittlung und der Rechtslage am anderen Ende ab. Dieser Grundsatz steht einer Online-Veröffentlichung nicht entgegen,

auch wenn dadurch Informationen außerhalb des EWR verfügbar werden. Wenn die Veröffentlichung in anderer Hinsicht mit dem DSG übereinstimmt (oder als im öffentlichen Interesse liegend ausgenommen ist), ist es angemessen, sie weltweit zu veröffentlichen" (ICO, 26).

Was ist, wenn Journalisten in einem Mitgliedstaat ansässig sind, aber Inhalte in anderen Ländern oder im Internet veröffentlichen wollen? In der Datenschutz-Grundverordnung heißt es: "Weichen solche Ausnahmen oder Abweichungen von einem Mitgliedstaat zum anderen ab, sollte das Recht des Mitgliedstaats gelten, dem der für die Verarbeitung Verantwortliche unterliegt". Dies könnte zu merkwürdigen Konsequenzen führen. So könnte beispielsweise eine Veröffentlichung eines in Spanien ansässigen Verlegers (oder Bloggers) von den dortigen relativ laxen Vorschriften zum Schutz der Privatsphäre von "Prominenten" profitieren, selbst wenn die betreffende Veröffentlichung bei einem französischen Verleger verboten wäre und obwohl die spanische Veröffentlichung von Frankreich aus leicht (und direkt online) zugänglich ist. Darüber hinaus könnten sie sogar davon profitieren, dass sie ihren Sitz in Spanien haben, selbst wenn die Veröffentlichung in französischer Sprache erfolgt und an ein französisches Publikum gerichtet ist. Dieser kurze Hinweis auf das anwendbare Recht ist für die Online-Umgebung unzureichend. Solange dies nicht in der Nachfolgeregelung der Datenschutzrichtlinie für elektronische Kommunikation genauer behandelt wird, könnte das rechtliche Umfeld für die freie Meinungsäußerung sehr unklar werden, insbesondere im digitalen Online-Umfeld (EDRI, 51).

4. Anwendung der Datenschutz-Grundverordnung auf den Journalismus

4.1 Die Datenschutz-Grundverordnung in aller Kürze

Die Datenschutz-Grundverordnung soll die Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, den wirtschaftlichen und sozialen Fortschritt, die Stärkung und Konvergenz der Volkswirtschaften im Binnenmarkt und das Wohlergehen der natürlichen Personen fördern (Erwägungsgrund 2). Sie zielt darauf ab, ein angemessenes Gleichgewicht zwischen dem

Datenschutz und dem Schutz der Privatsphäre und einigen anderen Grundrechten, wie z. B. dem Recht auf freie Meinungsäußerung, zu gewährleisten.

Die Verordnung konzentriert sich hauptsächlich auf die Verarbeitung personenbezogener Daten, d. h. "alle Informationen über eine bestimmbare lebende Person, die auf einem Computer oder einem anderen digitalen Gerät gespeichert sind (oder werden) oder in einem organisierten Ablagesystem abgelegt sind, in dem sie leicht gefunden werden können" (ICO, 2). Es geht also um strukturierte Daten, die Informationen über eine lebende Person enthalten. Handschriftliche Notizen gelten beispielsweise nicht als personenbezogene Daten. Wenn jedoch jemand diese Notizen auf einen Computer überträgt und sie organisiert, werden sie zu personenbezogenen Daten.

Ebenso sind anonymisierte Informationen keine personenbezogenen Daten, sollten aber nicht mit pseudonymisierten Informationen verwechselt werden, d. h. mit Informationen, die mit einer Person in Verbindung gebracht werden könnten (siehe die Begriffsbestimmung unten). Informationen, die sich auf verstorbene Personen beziehen, sind ebenfalls nicht durch die DSGVO geschützt, auch wenn ihre Veröffentlichung zu Problemen im Zusammenhang mit dem Recht auf Ehre oder dem öffentlichen Ansehen führen kann. Andererseits ändert die Tatsache, dass ein Teil der Daten öffentlich oder privat ist, nichts an seinem Charakter als personenbezogene Daten. Sie kann jedoch Auswirkungen auf die Rechtmäßigkeit ihrer Verarbeitung haben.

4.2 Die Rechtsgrundlagen für die Datenverarbeitung

Im Allgemeinen dürfen personenbezogene Daten nur auf einer Rechtsgrundlage verarbeitet werden. In Artikel 6 der Verordnung werden bis zu sechs Rechtsgrundlagen für eine rechtmäßige Verarbeitung genannt, nämlich:

1. die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat
2. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung von Maßnahmen erforderlich, die auf Antrag der betroffenen Person vor Abschluss eines Vertrags erfolgen
3. die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt

4. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen
5. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde
6. die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt.

Es gibt drei Rechtsgrundlagen für die Verarbeitung, die in der Regel für Journalisten gelten. Diese sind die Einwilligung, das öffentliche Interesse und das berechtigte Interesse. Sie werden in Abschnitt 5.3 näher erläutert.

4.3 Die besonderen Kategorien von Daten

Einige Daten sind durch die Datenschutz-Grundverordnung besonders geschützt und Journalisten müssen äußerst vorsichtig sein, wenn sie bereit sind, diese zu verarbeiten. Zu diesen besonderen Kategorien gehören: Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Mitgliedschaft in einer Gewerkschaft hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten über Gesundheit oder Daten über das Sexualleben oder die sexuelle Ausrichtung einer natürlichen Person.

Ein für die Verarbeitung Verantwortlicher darf solche Daten nur verarbeiten, wenn er eine rechtliche Grundlage für das Vorgehen gemäß Artikel 6 der DSGVO hat und einer der Umstände vorliegt, die das Verbot der Verarbeitung gemäß Artikel 9.1 abmildern. Diese Umstände sind in Artikel 9.2 der DSGVO aufgeführt. Grundsätzlich scheinen die ausdrückliche Zustimmung des Betroffenen, der die Informationen zur Verfügung stellt, oder die öffentliche Bekanntgabe durch die Personen, auf die sich die Informationen beziehen, die vielversprechendsten Umstände zu sein. Der für die Verarbeitung Verantwortliche muss jedoch stets bedenken, dass er diese besonders sensiblen Daten nur dann offenlegen sollte, wenn ein erhebliches öffentliches Interesse besteht. In der folgenden Tabelle finden Sie eine Zusammenstellung des EGMR in den Guidelines on Safeguarding Privacy in the Media, die die Rechtsprechung des EGMR zusammenfasst

Diesbezüglich hat das ICO erklärt, dass "wenn es sich bei den Informationen um 'sensible personenbezogene Daten' handelt, Organisationen auch eine der folgenden Bedingungen erfüllen müssen:

- die Person hat ihre ausdrückliche Zustimmung gegeben
- die Informationen wurden bereits durch Schritte, die eine Person bewusst unternommen hat, öffentlich gemacht. Es reicht nicht aus, dass sie bereits öffentlich zugänglich sind - es muss die betroffene Person sein, die die Schritte unternommen hat, die sie öffentlich gemacht haben" (ICO, 41).

4.4 Die Rechte der betroffenen Person und die Pflichten des für die Verarbeitung Verantwortlichen

Schließlich ist es wichtig zu erwähnen, dass die DSGVO der betroffenen Person einige grundlegende Rechte einräumt, die eingehalten werden müssen, sofern keine Ausnahmen und Befreiungen gelten. Dazu gehören:

- das Recht auf Auskunft. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht, und, falls dies der Fall ist, Zugang zu den personenbezogenen Daten sowie Informationen über die Zwecke der Verarbeitung, die betroffenen Kategorien personenbezogener Daten, die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben wurden oder werden, usw. (siehe Artikel 15 der Datenschutz-Grundverordnung).

- Das Recht auf Berichtigung. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen ohne unangemessene Verzögerung die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen.

- Recht auf Löschung ("Recht auf Vergessenwerden"). Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der für die Verarbeitung Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, wenn die in Artikel 17 der DSGVO aufgeführten Umstände vorliegen.

- Recht auf Einschränkung der Verarbeitung. Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für einen Zeitraum, der es

dem für die Verarbeitung Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen, oder wenn die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung ihrer Nutzung verlangt; oder der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr benötigt, sie aber von der betroffenen Person zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden; oder die betroffene Person Widerspruch gegen die Verarbeitung gemäß Artikel 21 Absatz 1 eingelegt hat, solange nicht geprüft wurde, ob die berechtigten Gründe des für die Verarbeitung Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

- Recht auf Datenübertragbarkeit. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Darüber hinaus hat der für die Verarbeitung Verantwortliche nach der Datenschutz-Grundverordnung zwei wesentliche Pflichten zu erfüllen:

- die Pflicht, der betroffenen Person Informationen zur Verfügung zu stellen, unabhängig davon, ob diese bei ihr erhoben wurden oder nicht. Dazu gehören Informationen über die Identität und die Kontaktdaten des für die Verarbeitung Verantwortlichen und gegebenenfalls des Vertreters des für die Verarbeitung Verantwortlichen, die Kontaktdaten des Datenschutzbeauftragten, gegebenenfalls die Zwecke der Verarbeitung, für die die personenbezogenen Daten bestimmt sind, sowie die Rechtsgrundlage für die Verarbeitung usw. (siehe Artikel 13 und 14 der DSGVO)

- Meldepflicht für die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung. Der für die Verarbeitung Verantwortliche hat die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung jedem Empfänger mitzuteilen, dem die personenbezogenen Daten offengelegt wurden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

4.5 Die wichtigsten Konzepte

Es gibt mehrere Begriffe, die im Zusammenhang mit der Datenschutz-Grundverordnung besonders relevant sind und deren Bedeutung Journalisten kennen müssen. Diese sind:

- „Personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt

oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

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

- „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

- „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

- Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

- „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personen- bezogene Daten im Auftrag des Verantwortlichen verarbeitet;

- „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

- „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

- „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissver- ständlich 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;

5. Die auf den Journalismus angewandten Grundsätze

5.1 Einleitung

Dieser Abschnitt soll Journalisten einige konkrete Tipps für ihre tägliche Arbeit geben. Es wird eine leicht verständliche, einfache Sprache verwendet, die auch von einem Nicht-Experten verstanden werden kann. Er ist auf der Grundlage der in der Datenschutz-Grundverordnung festgelegten Grundsätze aufgebaut. Dies ist auf eine einfache Tatsache zurückzuführen: Die Verarbeitung muss immer unter Beachtung dieser Grundsätze erfolgen, die den Kern der DSGVO bilden. Das bedeutet, dass Sie, auch wenn Sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten haben, diese Grundprinzipien einhalten müssen. Andernfalls wäre Ihre Verarbeitung nicht rechtmäßig.

Auf den folgenden Seiten zeigen wir diese Grundsätze auf und geben Ratschläge für den Umgang mit ihnen aus der Perspektive eines Journalisten. Diese Ratschläge basieren auf den Empfehlungen des Europarats in seinen Leitlinien zum Schutz der Privatsphäre in den Medien, die im Juni 2018 gemeinsam vom Lenkungsausschuss für Medien und Informationsgesellschaft (CDMSI) und dem Ausschuss der Konvention 108 (Datenschutzkonvention des Europarats) verabschiedet wurden. Diese Leitlinien umfassen eine Sammlung von Standards des Europarats (der Rat/CoE) und des Europäischen Gerichtshofs für Menschenrechte (der Gerichtshof) zum Schutz der Privatsphäre von Personen des öffentlichen Lebens und Privatpersonen in den Medien. **Bitte denken Sie immer daran, dass dieser Teil des Handbuchs vor allem**

Anleitungen für den Umgang mit den von der Datenschutz-Grundverordnung angenommenen Grundsätzen aus ethischer Sicht enthält. Um eine angemessene Rechtskonformität zu gewährleisten, müssen Sie die von dem jeweiligen Mitgliedstaat erlassenen Vorschriften befolgen.

5.2 Rechtmäßigkeit, Fairness und Transparenz

Gemäß Artikel 5 Absatz 1 Buchstabe a der Datenschutz-Grundverordnung müssen "personenbezogene Daten rechtmäßig, nach Treu und Glauben und in einer gegenüber der betroffenen Person transparenten Weise verarbeitet werden". Dieser Grundsatz umfasst drei verschiedene Anforderungen.

- Rechtmäßigkeit. Die Datenverarbeitung ist nur dann rechtmäßig, wenn eine Legitimationsgrundlage sie erlaubt (siehe Abschnitt 3.1). Bei den meisten Informationen, die ein Journalist sammelt, handelt es sich um personenbezogene Daten. Daher bedeutet die Beschaffung von Informationen häufig eine Datenverarbeitung und sollte daher den Grundsätzen der Datenschutz-Grundverordnung entsprechen. Das bedeutet, dass Sie über eine Rechtsgrundlage für die Verarbeitung der Daten verfügen müssen und die Gründe für die Erhebung der Daten begründen müssen.

- Fairness. Das Konzept der Fairness ist schwer zu definieren. Er bezieht sich auf die Tatsache, dass die Verarbeitung mit dem Geist der DSGVO übereinstimmen muss, nicht nur mit ihrem Wortlaut. Auf diese Weise können die Bestimmungen anderer Vorschriften, die für die Definition dessen, was in der EU und ihren Mitgliedstaaten als "fair" gilt, von besonderer Bedeutung sind, wie etwa die EU-Grundrechtecharta, in die Anwendung der Datenschutz-Grundverordnung einbezogen werden. Generell kann man jedoch sagen, dass Fairness bedeutet, dass die Informationen in einer Weise verarbeitet werden, die den rationalen Erwartungen der betroffenen Personen entspricht. Die ICO hat erklärt, dass Fairness bedeutet, dass "die Medien, wo immer möglich, Informationen über Personen auf faire und rechtmäßige Weise sammeln und verwenden und keinen ungerechtfertigten Schaden verursachen sollten. Journalisten werden oft in der Lage sein, Informationen ohne das Wissen oder die Zustimmung der betroffenen Person zu sammeln, aber es ist unfair, Menschen aktiv über die Identität oder die Absichten des Journalisten in die Irre zu führen" (ICO, 40).

- Transparenz. Mit dem Grundsatz der Transparenz soll sichergestellt werden, dass alle interessierten Parteien über jede Verarbeitung ihrer personenbezogenen Daten Bescheid wissen und dass sie Zugang zu wesentlichen Informationen über deren spezifischen Inhalt haben. Im Allgemeinen sollten Sie auch der Person, bei der Sie die Informationen erheben, und der Person, über die sich die Informationen beziehen (d. h. der betroffenen Person), mitteilen, wer Sie sind und was Sie mit ihren Informationen tun. Wenn sie Ihnen die Informationen für einen bestimmten Zweck zur Verfügung stellen, sollten Sie sie nicht für einen

anderen Zweck verwenden. Manchmal könnte die Benachrichtigung der betroffenen Personen über die Datenverarbeitung die journalistische Tätigkeit beeinträchtigen. Manchmal verwenden Sie aufdringliche, verdeckte Methoden, um an eine Story zu kommen, z. B. Überwachung. All diese Umstände können akzeptabel sein, solange es keine Alternative gibt, die mit den Datenschutzgrundsätzen besser vereinbar ist, und die Geschichte von öffentlichem Interesse ist. Und genau das ist der springende Punkt: Sie können die betroffene Person nur dann nicht über die Verarbeitung informieren, wenn dies die Ausübung des Journalismus unmöglich machen würde. Mit anderen Worten: Sie müssen die betroffenen Personen über die Verarbeitung informieren, es sei denn, Sie sind der Ansicht, dass Sie sonst nicht in der Lage wären, die Geschichte zu schreiben. Sobald dies nicht mehr zutrifft, sollten Sie die in der Datenschutz-Grundverordnung festgelegten Verpflichtungen einhalten. Wie das ICO erklärte, "akzeptieren wir, dass es für Journalisten im Allgemeinen nicht praktikabel ist, mit allen Personen, über die sie Informationen sammeln, Kontakt aufzunehmen. Oft wird es fair sein, Informationen über Angelegenheiten von potenziellem journalistischem Interesse ohne das Wissen der Person zu sammeln. Es wird jedoch Fälle geben, in denen es aus Gründen der Fairness erforderlich ist, direkten Kontakt mit dem Gegenstand einer größeren Untersuchung aufzunehmen, um ihm die Möglichkeit zu geben, seine Sicht der Dinge darzulegen" (ICO, 40).

5.3 Wahl einer Rechtsgrundlage für die Verarbeitung

Es gibt drei Rechtsgrundlagen für die Verarbeitung, die normalerweise für den Journalismus gelten. Dies sind die Einwilligung, das öffentliche Interesse und das berechtigte Interesse.

Einverständnis. Daten können verarbeitet werden, wenn die Personen, auf die sich die Informationen beziehen, ihre Zustimmung gegeben haben. Wenn sich die Informationen auf mehrere Personen beziehen, sollten alle Personen ihre Zustimmung geben. Die Einwilligung muss frei, konkret und in Kenntnis der Sachlage gegeben werden. Es ist hervorzuheben, dass die bloße Tatsache, dass jemand personenbezogene Daten auf einer öffentlichen Website, wie z. B. seinem Facebook-Profil, veröffentlicht hat, nicht bedeutet, dass diese Daten ohne seine Zustimmung oder eine andere Rechtsgrundlage verwendet werden können. Die Einwilligung muss sich auf die Zwecke der Datenverarbeitung erstrecken. Wenn Sie also die Daten für einen anderen als den ursprünglich von der betroffenen Person gewünschten Zweck verwenden wollen, benötigen Sie eine Rechtsgrundlage. Es kann Ausnahmen von dieser Regel geben, insbesondere wenn es sich bei der betroffenen Person um eine Person des öffentlichen Lebens handelt, aber unter diesen Umständen sollten Sie die Daten auf der Grundlage

des berechtigten Interesses und nicht auf der Grundlage der Einwilligung verarbeiten. In den Leitlinien zum Schutz der Privatsphäre in den Medien heißt es: "Journalisten sollten grundsätzlich die Zustimmung der betroffenen Person zum Zeitpunkt der Aufnahme des Bildes einholen und nicht erst, wenn es veröffentlicht wird. Andernfalls ist ein wesentliches Merkmal der Persönlichkeit (das Bild) von Dritten abhängig und die betroffene Person hat keine Kontrolle darüber" (S. 20).

Öffentliches Interesse. Daten können verarbeitet werden, wenn sie für die Erfüllung einer Aufgabe im öffentlichen Interesse erforderlich sind. Dies ist in der Tat die empfehlenswerteste Rechtsgrundlage, wenn Sie zu einer öffentlichen Einrichtung gehören, die als solche tätig ist (wenn keine Einwilligung vorliegt). Wenn Sie ein privater Akteur sind oder eine öffentliche Einrichtung, die als privater Akteur tätig ist, ist die Grundlage des berechtigten Interesses empfehlenswerter. Dies ist darauf zurückzuführen, dass das öffentliche Interesse die Verarbeitung nicht legitimieren kann, wenn die Interessen der betroffenen Person nicht berücksichtigt werden, da Information kein absolutes Recht oder keine absolute Pflicht ist. Wenn dies jedoch der Fall ist, sind das berechtigte Interesse und die Abwägung Konzepte, die sehr gut mit der Verarbeitung funktionieren. Daher ist es empfehlenswert, das berechtigte Interesse als Rechtsgrundlage für die Verarbeitung zu verwenden.

Legitimes Interesse. Die Verarbeitung ist für "berechtigte Interessen" erforderlich, vorausgesetzt, dass sie der betroffenen Person keinen ungerechtfertigten Schaden zufügen wird. "Zu den berechtigten Interessen gehören die kommerziellen und journalistischen Interessen eines Medienunternehmens an der Sammlung und Veröffentlichung von Material sowie das öffentliche Interesse an der freien Meinungsäußerung und dem Recht auf Wissen. Es handelt sich also um eine umfassende Rechtsgrundlage, die das öffentliche Interesse, aber nicht nur das öffentliche Interesse umfasst. Um alle beteiligten Interessen gegeneinander abzuwägen, sollten Sie ein Verfahren anwenden, das sicherstellt, dass das berechtigte Interesse als Rechtsgrundlage für die Verarbeitung dient und drei Hauptphasen umfasst (Detrekői):

- Zunächst müssen Sie ein berechtigtes Interesse nachweisen (warum die Geschichte dem öffentlichen Interesse dient).

- zweitens müssen Sie eine Erforderlichkeitsprüfung durchführen (inwieweit die Veröffentlichung von Namen und personenbezogenen Daten erforderlich ist, um den Artikel informativ zu gestalten)
- Schließlich müssen Sie eine Abwägung vornehmen, um nachzuweisen, dass das Interesse der Öffentlichkeit, über das in dem Bericht behandelte Thema informiert zu werden, das Interesse des Einzelnen, seine persönlichen Daten vor der Öffentlichkeit zu verbergen, überwiegt. Je größer der Informationswert für die Öffentlichkeit ist, desto mehr muss das Interesse einer Person, vor der Veröffentlichung geschützt zu werden, zurückstehen und umgekehrt (Guidelines on Safeguarding Privacy in the Media, S.11).

Eine ausführliche Beschreibung einer Abwägungsprüfung ist in Anhang I dieses Dokuments enthalten. Die Rechtsprechung des EGMR ist recht umfangreich zum Gleichgewicht zwischen öffentlichem Interesse und Privatsphäre (siehe Recht auf Schutz des eigenen Bildes, unter: https://www.echr.coe.int/documents/fs_own_image_eng.pdf). Eine hervorragende Zusammenfassung seines Standpunkts findet sich in der Rechtssache Kaboğlu und Oran gegen die Türkei: "In mehreren seiner Urteile hat der Gerichtshof die maßgeblichen Kriterien für die Abwägung zwischen dem Recht auf Achtung des Privatlebens und dem Recht auf freie Meinungsäußerung wie folgt zusammengefasst: Beitrag zu einer Debatte von öffentlichem Interesse, Bekanntheit der betreffenden Person, Gegenstand der Berichterstattung, vorheriges Verhalten der betreffenden Person, Inhalt, Form und Folgen der Veröffentlichung sowie gegebenenfalls die Umstände des Falles (siehe *Von Hannover* (Nr. 2) [GC], a.a.O., §§ 108-113, und *Axel Springer AG*, a.a.O., §§ 89-95; siehe auch *Couderc und Hachette Filipacchi Associés*, a.a.O., § 93). Wenn die beiden fraglichen Rechte in einer Weise abgewogen wurden, die mit den von der Rechtsprechung des Gerichtshofs aufgestellten Kriterien übereinstimmt, bräuchte der Gerichtshof gewichtige Gründe, um seine Auffassung an die Stelle der Auffassung der innerstaatlichen Gerichte zu setzen (siehe *Palomo Sánchez u. a. gegen Spanien* [GC], Nr. 28955/06, 28957/06, 28959/06 und 28964/06, § 57, EGMR 2011)".

5.4 Zweckbindung

Personenbezogene Daten werden für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer Weise weiterverarbeitet, die mit diesen Zwecken unvereinbar ist. Dies bedeutet, dass die Daten nur für bestimmte Zwecke verarbeitet werden dürfen, die bei der Begründung der Verarbeitung ausdrücklich angegeben

werden müssen. Daher sollten Sie beispielsweise immer daran denken, dass Sie die Daten, die Sie in Ihren Unterlagen aufbewahren, nicht für andere Zwecke verwenden dürfen als die, die ihre Verarbeitung gerechtfertigt haben, es sei denn, Sie haben eine Grundlage, die als Grund für die neue Verarbeitung dient.

5.5 Minimierung der Datenmenge

Personenbezogene Daten müssen "den Zwecken entsprechen, für die sie erhoben werden, dafür erheblich sein und sich auf das beschränken, was im Hinblick auf die Zwecke, für die sie verarbeitet werden, erforderlich ist". Dieser Grundsatz besagt, dass "man genügend Informationen haben muss, um die Arbeit zu erledigen, aber nichts haben sollte, was man nicht wirklich braucht". Beachten Sie, dass dieser Grundsatz Ihren Zweck berücksichtigt. Da die Art des Journalismus das Sammeln und Abgleichen großer Mengen von Informationen erfordert, akzeptieren wir, dass Informationen ohne unmittelbare Relevanz für eine aktuelle Geschichte berechtigterweise für die zukünftige Verwendung aufbewahrt werden können, wenn sie sich auf eine Person oder ein Thema von allgemeinem journalistischem Interesse beziehen" (ICO, 25).

5.6 Genauigkeit

In Artikel 5 Absatz 1 Buchstabe d heißt es: "Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sein; es sind alle angemessenen Maßnahmen zu treffen, damit im Hinblick auf die Zwecke, für die sie verarbeitet werden, unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden.

Die Genauigkeit ist sowohl ein wesentlicher Grundsatz der Datenschutz-Grundverordnung als auch ein zentraler Wert des Journalismus. Daher sollten Journalisten besonders darauf achten, dass die veröffentlichten Informationen korrekt sind. Zu diesem Zweck müssen sie die Fakten überprüfen. Es kann argumentiert werden, dass nur korrekte Informationen gut mit der Idee der Förderung des öffentlichen Interesses zusammenpassen. Daher gelten die Ausnahmen und Abweichungen von Artikel 85 nur, wenn die Informationen korrekt sind. "Die Ausnahmeregelung kann jedoch in Anspruch genommen werden, wenn es sich

beispielsweise um einen Artikel handelt, der von dringendem öffentlichem Interesse ist, und wenn die kurze Frist eine vollständige Überprüfung der Richtigkeit sehr schwierig macht. Wie bei jeder Inanspruchnahme der Ausnahmeregelung müssen Sie nachweisen, dass jemand auf angemessener Ebene gründlich darüber nachgedacht hat, welche Überprüfungen möglich sind, ob die Veröffentlichung für weitere Überprüfungen aufgeschoben werden kann, welche Art von öffentlichem Interesse auf dem Spiel steht und dass die Entscheidung zur Veröffentlichung daher angemessen war" (ICO, 14).

Darüber hinaus setzt die Richtigkeit voraus, dass sehr angemessene Schritte unternommen werden, um sicherzustellen, dass personenbezogene Daten, die unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Dies ist von wesentlicher Bedeutung, da veröffentlichte Informationen das öffentliche Bild oder das Privatleben einer Person ernsthaft beeinträchtigen können. Laut Artikel 29 des Arbeitsdokuments müssen "das Recht auf Gegendarstellung und die Möglichkeit, falsche Informationen zu korrigieren, die beruflichen Pflichten von Journalisten und die mit ihnen verbundenen besonderen Selbstregulierungsverfahren sowie das Gesetz zum Schutz der Ehre (straf- und zivilrechtliche Bestimmungen über Verleumdung) bei der Bewertung des Schutzes der Privatsphäre in Bezug auf die Medien berücksichtigt werden" (A29WP, S. 7).

Daher müssen Journalisten besonders vorsichtig sein und die Informationen ändern, wenn sich herausstellt, dass sie die Realität nicht getreu wiedergeben. Dies muss natürlich besonders berücksichtigt werden, wenn die Personen, die die Berichtigung beantragen, die betroffenen Personen sind, gemäß ihrem Recht auf Berichtigung. Schließlich sollten Sie immer angeben, ob Sie eine Meinung äußern oder über eine Tatsache informieren. Dies ist wichtig, damit das Publikum die Informationen nicht falsch interpretiert.

5.6 Speicherbegrenzung

Der Grundsatz der Speicherbegrenzung bedeutet, dass Daten "so lange, wie es für die Erreichung der Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht" (Art. 5 DSGVO). Im Zusammenhang mit dem Journalismus bedeutet dies, dass Sie, sobald Sie Ihre Daten haben, einige Entscheidungen darüber treffen müssen, ob und wie lange Sie

sie speichern möchten. Daten sind für Journalisten sehr wertvoll, da sie oft als Hintergrundmaterial dienen können. Auch Kontaktdaten sind eine sehr wichtige Ressource, die Journalisten in der Regel aufbewahren möchten. Im Prinzip können Sie diese Daten für lange Zeit oder auf unbestimmte Zeit aufbewahren. Die Datenschutz-Grundverordnung sieht keine zeitliche Begrenzung für die Aufbewahrung personenbezogener Daten vor. Der Grundsatz der "Speicherbegrenzung" setzt lediglich voraus, dass es einen guten Grund für die Aufbewahrung der Daten gibt. Wenn dies der Fall ist, können sie auf unbestimmte Zeit aufbewahrt werden.

Wie die ICO jedoch feststellt (ICO, 12), "sollten Sie Ihre aufbewahrten Informationen von Zeit zu Zeit überprüfen, um sicherzustellen, dass die Angaben immer noch aktuell, relevant und nicht übermäßig für Ihre Bedürfnisse sind, und Sie sollten alle Angaben löschen, die Sie nicht mehr benötigen (z. B. wenn ein Kontakt seine Nummer geändert hat). Darüber hinaus sollte die Art und Weise, wie Sie die Informationen aufbewahren oder überprüfen, in den Organisationsrichtlinien festgelegt werden.

5.7 Integrität und Vertraulichkeit

Die Daten müssen "so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Beschädigung, durch geeignete technische oder organisatorische Maßnahmen gewährleistet ist" (Art. 5 DSGVO). Dieser Grundsatz zielt darauf ab, eine unbefugte oder unrechtmäßige Verarbeitung und einen zufälligen Verlust, eine zufällige Zerstörung oder eine zufällige Beschädigung der Daten zu verhindern.

Bei den von Ihnen gespeicherten Daten handelt es sich um sensibles Material. Daher müssen Sie Ihr Bestes tun, um zu verhindern, dass sie verloren gehen, gestohlen oder missbraucht werden. Versuchen Sie, sie zu schützen, indem Sie die von Ihrer Organisation festgelegten Verfahren und Sicherheitsprotokolle beachten. In der Tat sollten alle Mitarbeiter eines Medienunternehmens die Richtlinien und Verfahren des Unternehmens kennen und befolgen. Informationen sollten verschlossen, passwortgeschützt und nach Möglichkeit verschlüsselt werden. Sie müssen besonders

auf die Sicherheit achten, wenn Sie mit Dokumenten, Telefonen oder Laptops, die persönliche Daten enthalten, das Büro verlassen.

Der Umfang der erforderlichen Sicherheitsmaßnahmen ist nicht festgelegt. Grundsätzlich können Sicherheitsmaßnahmen angemessen sein, um sicherzustellen, dass kein unrechtmäßiger Zugriff erfolgt oder um versehentlichen Verlust, Zerstörung oder Beschädigung zu vermeiden. Journalisten sollten abwägen, wie sensibel oder vertraulich die Informationen sind, über die sie verfügen, wie groß der Schaden sein könnte, der durch den Verlust oder die missbräuchliche Verwendung der Informationen entsteht, welche Technologie zur Verfügung steht und welche Kosten damit verbunden sind. Die Sicherheitsvorkehrungen müssen nicht dem neuesten Stand der Technik entsprechen, aber sie sollten dem Risiko angemessen sein. Die Organisationen müssen technische (elektronische) und physische Sicherheitsmaßnahmen, Strategien und Verfahren sowie die Schulung und Überwachung des Personals in Betracht ziehen. Diese Maßnahmen sollten sich sowohl auf das innerhalb als auch auf das außerhalb des Büros arbeitende Personal beziehen. In jedem Fall sollten die Organisationen in der Lage sein, das gewählte Sicherheitsniveau zu rechtfertigen (ICO, 43).

5.8 Rechenschaftspflicht

Gemäß Artikel 5 Absatz 2 der DSGVO "ist der für die Verarbeitung Verantwortliche für die Einhaltung von Absatz 1 verantwortlich und muss in der Lage sein, dies nachzuweisen". Diese Klausel besagt, dass der für die Datenverarbeitung Verantwortliche nicht nur für die Einhaltung der DSGVO verantwortlich ist, sondern auch in der Lage sein sollte, diese Einhaltung nachzuweisen. Daher trägt der für die Verarbeitung Verantwortliche die Beweislast für die Einhaltung der DSGVO. Im Falle des Journalismus kann es vorkommen, dass tatsächlich eine Ausnahme von den Rechten der betroffenen Person gemacht wurde. In solchen Fällen sollten Organisationen oder Journalisten in der Lage sein zu erklären, warum die Einhaltung der einschlägigen Bestimmungen nicht mit den Zwecken des Journalismus vereinbar war. Zu diesem Zweck sollten sie häufig nachweisen, dass sie eine Abwägung der verschiedenen auf dem Spiel stehenden Interessen vorgenommen haben. Die Angabe, dass die Einhaltung der Vorschriften nicht branchenüblich ist, würde in jedem Fall nicht ausreichen. Das Führen eines Prüfpfads in Fällen, die umstritten sind oder sich als besonders umstritten

erweisen könnten, könnte ein geeignetes Instrument sein, um die Verantwortlichkeit zu demonstrieren.

Wie Biriukova feststellte, "muss das Medienunternehmen, ein Journalist oder im Grunde jeder, der sich auf die Ausnahmeregelung berufen möchte, erstens das öffentliche Interesse der beabsichtigten Veröffentlichung nachweisen und zweitens verstehen, welche Datenschutzverpflichtungen in diesem Fall mit den journalistischen Zwecken in Konflikt geraten würden. Wenn es um eine journalistische Untersuchung von Korruption in der Regierung geht, könnte eine Verweigerung der Offenlegung der Informationsquelle vielleicht leicht verteidigt werden, aber andere, weniger schwarz-weiße Szenarien (z. B. Meldungen über Datenschutzverletzungen) können zu Problemen bei der Einhaltung der Vorschriften führen. Gleichzeitig ist es schwer vorstellbar, dass z. B. ein Bürgerjournalist von vornherein eine solche Abwägung vornehmen würde. Solange keine detaillierteren Leitlinien, Verfahrens- oder Verhaltenskodizes zur Verfügung gestellt werden, besteht die Gefahr, dass ein solch nuancierter Ansatz weitgehend theoretisch und nicht praktikabel bleibt" (Biriukova, 22).

Wir sollten auch immer bedenken, dass der für die Datenverarbeitung Verantwortliche im Allgemeinen nicht ein einzelner Journalist ist, sondern die Organisation, in der er oder sie arbeitet. Daher ist die Organisation für die Umsetzung von organisatorischen Maßnahmen und Strategien in Bezug auf die Datenverarbeitung und die Verantwortung verantwortlich. Die Organisation muss nämlich nachweisen können, dass die Verarbeitung der Daten das Endergebnis eines Entscheidungsprozesses war, bei dem alle in Frage kommenden Aspekte berücksichtigt wurden. Die Verfahren können je nach Art der Organisation und der Informationen sehr unterschiedlich sein, doch sollte es in jeder Organisation eine Art strukturiertes Verfahren geben. Darüber hinaus wäre es gut, einige Verhaltenskodizes im Rahmen des Journalistenberufs in jedem Mitgliedstaat zu entwickeln. Die Artikel-29-Datenschutzgruppe stellte fest, dass "bei der Bewertung, ob Ausnahmen oder Abweichungen verhältnismäßig sind, die bestehenden ethischen und beruflichen Verpflichtungen der Journalisten sowie die Formen der Selbstkontrolle des Berufsstandes berücksichtigt werden müssen" (A29WP, S.8).

Wie die ICO feststellt, "kann es bei vielen alltäglichen Geschichten durchaus angemessen sein, dass der Journalist sein eigenes Urteilsvermögen einsetzt, aber bei aufsehenerregenden, aufdringlichen oder schädlichen Geschichten ist wahrscheinlich eine stärkere redaktionelle Beteiligung und eine formellere Abwägung des öffentlichen Interesses erforderlich. Die Organisationspolitik sollte dazu dienen, zu erklären, wann eine stärkere redaktionelle Beteiligung erforderlich ist. Unserer Ansicht nach ist die Überzeugung zum Zeitpunkt der Verarbeitung ausschlaggebend. Der für die Verarbeitung Verantwortliche muss nachweisen können, dass er von dem öffentlichen Interesse überzeugt war, d. h., dass die Frage des öffentlichen Interesses tatsächlich geprüft wurde. Er sollte auch nachweisen können, dass diese Überlegung zum Zeitpunkt der betreffenden Verarbeitung personenbezogener Daten angestellt wurde und nicht erst im Nachhinein. Wenn ein Journalist zunächst davon ausgeht, dass eine Geschichte im öffentlichen Interesse liegt, die Organisation aber schließlich beschließt, sie nicht zu veröffentlichen, kann die Ausnahmeregelung immer noch für alle bis zu diesem Zeitpunkt durchgeführten journalistischen Tätigkeiten gelten.

Zweitens erfordert die Ausnahmeregelung nur eine begründete Überzeugung. Dies lässt viel mehr Spielraum als andere Ausnahmen und spiegelt die Bedeutung freier und unabhängiger Medien wider (ICO, 35). Die folgende Tabelle zeigt einige Maßnahmen in den Leitlinien zum Schutz der Privatsphäre in den Medien, die für Organisationen, die die Einhaltung des Datenschutzes gewährleisten wollen, von Nutzen sein könnten.

6. Zusätzliche Fragen

6.1 Anträge auf Zugang zu Dokumenten

Der Zugang zu den von Journalisten gespeicherten Informationen kann sehr wichtig sein, sowohl für die Themen, über die sie berichten, als auch für andere Personen. Erstere haben jedoch ein Recht auf Zugang, das andere nicht haben. Artikel 85 erlaubt es den Mitgliedstaaten jedoch, dieses Recht zu beschränken. In diesem Abschnitt werden wir einige Überlegungen dazu anstellen, wie diese Einschränkung normalerweise formuliert wird. Dabei werden wir uns sowohl auf das Recht auf Zugang als auch auf das Recht auf Nichtweitergabe der Informationsquellen konzentrieren, die in Europa weithin anerkannt sind.

Gemäß Artikel 15 der Datenschutz-Grundverordnung hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten verarbeitet werden oder nicht; ist dies der Fall, so hat sie das Recht auf Auskunft über die personenbezogenen Daten und auf Informationen über die Zwecke der Verarbeitung, die betroffenen Datenkategorien, die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben wurden oder werden, insbesondere Empfänger in Drittländern oder internationale Organisationen, die vorgesehene Dauer der Speicherung der personenbezogenen Daten, usw.

Auf dieser Grundlage sollte ein Journalist den betroffenen Personen die Informationen, die er über sie besitzt, zur Verfügung stellen, es sei denn, er ist der Ansicht, dass er sonst nicht in der Lage wäre, die Geschichte zu schreiben. Unter diesen Umständen würden die Ausnahmen und Abweichungen von Artikel 85 gegenüber dem Recht auf Auskunft Vorrang haben. Dies würde natürlich nur unter der Voraussetzung geschehen, dass die Geschichte von öffentlichem Interesse ist. Je höher das Interesse ist, desto stärker ist das Recht, die Informationen nicht an die betroffene Person weiterzugeben. Häufig kann es vorkommen, dass Sie Zugang zu einigen Informationen über die Verarbeitung oder die verwendeten personenbezogenen Daten gewähren können, ohne dass die Ziele Ihrer Untersuchung dadurch beeinträchtigt werden. Wenn dies der Fall ist, sollten Sie unverzüglich fortfahren.

Die Verweigerung der angeforderten Informationen kann durchaus gerechtfertigt sein, auch wenn die Geschichte bereits veröffentlicht wurde. Wenn Sie triftige Gründe für die Annahme haben, dass dies gegen das öffentliche Interesse verstößt, und wenn Sie erklären können, warum die Beantwortung des Ersuchens künftige Untersuchungen oder Veröffentlichungen oder die journalistische Tätigkeit im Allgemeinen beeinträchtigen würde, können Sie das Ersuchen ablehnen. Sie müssen jedoch immer einen guten Grund für die Ablehnung anführen. Vergessen Sie nicht, dass Sie keine Informationen über andere Personen weitergeben dürfen, es sei denn, diese haben zugestimmt oder es ist vertretbar, sie ohne ihre Zustimmung weiterzugeben.

6.2 Vertrauliche Quellen

Informationsquellen sind für Journalisten heilig. Mehrere internationale Instrumente gewährleisten ihren angemessenen Schutz, darunter die Entschließung zu den journalistischen Freiheiten und den Menschenrechten, die auf der 4th. Europäischen Ministerkonferenz zur Massenmedienpolitik (Prag, 7.-8. Dezember 1994) angenommen wurde, und die Entschließung des Europäischen Parlaments zur Vertraulichkeit von Journalistenquellen (18. Januar 1994, Amtsblatt der Europäischen Gemeinschaften Nr. C 44/34). Darüber hinaus hat das Ministerkomitee des Europarats am 8. März 2000 die Empfehlung Nr. R(2000) 7 über das Recht von Journalisten, ihre Informationsquellen nicht preiszugeben, angenommen. Darüber hinaus sehen das innerstaatliche Recht und die Praxis in den Mitgliedstaaten im Allgemeinen einen ausdrücklichen und eindeutigen Schutz des Rechts von Journalisten vor, Informationen zur Identifizierung einer Quelle gemäß Artikel 10 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten nicht offen zu legen.

Es gibt also einen rechtlichen Rahmen, der es Journalisten erlaubt, ihre Quellen geheim zu halten. Dieses Recht kann nur unter den in Grundsatz 3(b) der Empfehlung Nr. R(2000) 7 genannten Bedingungen eingeschränkt werden, nämlich:

> "i. es keine angemessenen alternativen Maßnahmen zur Offenlegung gibt oder diese von den Personen oder Behörden, die die Offenlegung wünschen, ausgeschöpft wurden, und
>
> ii. das berechtigte Interesse an der Bekanntgabe das öffentliche Interesse an der Nichtbekanntgabe eindeutig überwiegt, wobei zu berücksichtigen ist, dass:
>
> -ein zwingendes Erfordernis für die Notwendigkeit der Offenlegung nachgewiesen wird,
>
> -Die Umstände sind hinreichend vital und schwerwiegend,
>
> -die Notwendigkeit der Offenlegung als Reaktion auf ein dringendes gesellschaftliches Bedürfnis erkannt wird, und

-Mitgliedstaaten verfügen bei der Beurteilung dieser Notwendigkeit über einen gewissen Ermessensspielraum, der jedoch mit der Kontrolle durch den Europäischen Gerichtshof für Menschenrechte einhergeht.

c. Die oben genannten Anforderungen sollten in allen Phasen eines Verfahrens angewandt werden, in denen das Recht auf Geheimhaltung geltend gemacht werden könnte".

Schließlich dürfen wir nicht vergessen, dass die Offenlegung einer Quelle auch eine Datenverarbeitung impliziert. Und dass die Quelle auch eine betroffene Person ist, die über die Rechte verfügt, die ihr durch die DSGVO verliehen werden. Wenn es sich bei der Quelle also um eine natürliche Person handelt, werden Sie wahrscheinlich in der Lage sein, ihre Identität auf der Grundlage der Datenschutz-Grundverordnung zu wahren. Wenn die betroffene Person einen Antrag auf Zugang zu den Daten stellt und diesem nur durch Offenlegung der Identität Ihrer Quellen entsprochen werden kann, können Sie nur fortfahren, wenn die Quelle zustimmt oder wenn dies unter Berücksichtigung aller Umstände angemessen ist. Handelt es sich bei der Quelle um eine Organisation, ändern sich die Umstände, da Organisationen nicht über personenbezogene Daten verfügen. Journalisten müssen sich also auf die Ausnahmeregelung für Journalisten berufen, um die Identität der Quelle zurückzuhalten, wenn diese nicht bereit ist, ihren Namen preiszugeben, oder wenn es nicht angemessen ist, ihn preiszugeben.

6.3 Minderjährige und schutzbedürftige Personen

Sie müssen besonders vorsichtig sein, wenn Sie Daten über Minderjährige oder schutzbedürftige Personengruppen verarbeiten wollen. Erstens könnte die Rechtsgrundlage für eine solche Verarbeitung nicht ausreichend sein. Die Einwilligung eines Minderjährigen ist nur dann gültig, wenn der Minderjährige sie gemäß dem Rechtsrahmen des Mitgliedstaats erteilen kann. Die Datenschutz-Grundverordnung legt ein Mindestalter fest, aber die Mitgliedstaaten sind befugt, dieses anzuheben. Daher müssen Sie sich darüber informieren. Wenn der Minderjährige oder die schutzbedürftige Person nicht in der Lage ist, seine Zustimmung zu geben, sollten seine gesetzlichen Vertreter die Zustimmung erteilen.

Wenn Sie keine Einwilligung in Kenntnis der Sachlage einholen können, sollte die Verarbeitung auf der Grundlage des berechtigten Interesses erfolgen. Das von dem für die Verarbeitung Verantwortlichen verfolgte berechtigte Interesse gilt jedoch nicht, "wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn die betroffene Person ein Kind ist". Daher ist es höchst unwahrscheinlich, dass die Abwägungsprüfung die Verarbeitung personenbezogener Daten von Minderjährigen zulässt. Unserer Meinung nach gelten ähnliche Überlegungen auch für gefährdete Bevölkerungsgruppen.

Die Leitlinien zum Schutz der Privatsphäre in den Medien enthalten eine Zusammenfassung von zwei Fällen, die Minderjährige betreffen.

- "In der Rechtssache Kahn gegen Deutschland wurden Bilder von zwei Kindern von Oliver Kahn, einem ehemaligen Torwart der deutschen Fußballnationalmannschaft, und seiner Frau in einer Zeitschrift abgebildet. Die Journalisten wurden zu einer Geldstrafe verurteilt, weil sie das Recht der Familie auf Privatsphäre verletzt hatten. Alle Fotos zeigten die Kinder in Begleitung ihrer Eltern oder im Urlaub, obwohl das Thema der Berichterstattung nicht die Kinder selbst, sondern die Beziehung der Eltern und die Karriere von Oliver Kahn war.
- In der Rechtssache Reklos und Davourlis gegen Griechenland wurde die Aufnahme von Bildern eines Neugeborenen ohne die Zustimmung seiner Eltern (auf der Intensivstation, zu der nur das Krankenhauspersonal Zugang haben sollte) als Verletzung des Rechts auf Privatsphäre angesehen, obwohl die Bilder nicht veröffentlicht wurden".

Beachten Sie, dass dieser letzte Satz besonders wichtig ist, da er sich auf die Notwendigkeit einer Rechtsgrundlage für die Datenverarbeitung zu dem Zeitpunkt konzentriert, zu dem die Fotos gemacht werden. Die Entscheidung, sie nicht zu veröffentlichen, verhindert nur eine spätere unrechtmäßige Verarbeitung (Veröffentlichung), heilt aber nicht die vorherige Verletzung des Rechts auf Privatsphäre.

6.4 Mitnahmeeffekte

Es gibt einige Tipps, die als Zusammenfassung der Dinge dienen können, die Sie über die Einhaltung des Datenschutzes wissen müssen. Im Allgemeinen sollten Sie immer daran denken, dass:

- Die Veröffentlichung von personenbezogenen Daten bedeutet Datenverarbeitung. Daher müssen Sie sicher sein, dass Sie diese Daten veröffentlichen dürfen, bevor Sie dies tun. Zu diesem Zeitpunkt müssen Sie eine Rechtsgrundlage haben, die die Verarbeitung erlaubt. Andernfalls wäre sie unrechtmäßig.

- Wenn die personenbezogenen Daten verarbeitet werden, um dem öffentlichen Interesse zu dienen ("journalistische Zwecke"), ist es wahrscheinlich, dass die Verarbeitung nicht mit einigen oder allen Artikeln der DSGVO übereinstimmen muss. Umgekehrt bedeutet dies, dass die DSGVO in vollem Umfang gilt, wenn personenbezogene Daten aus anderen Gründen erhoben, analysiert oder anderweitig verarbeitet werden.

- Die Veröffentlichung sensibler Informationen könnte das Privatleben der betroffenen Person erheblich beeinträchtigen. Sie müssen sicher sein, dass der Nutzen für das öffentliche Interesse eine solche Beeinträchtigung rechtfertigt. Zu diesem Zweck sollten Sie die auf dem Spiel stehenden Interessen gegeneinander abwägen und dabei verschiedene Grade des Eingriffs in das Privatleben der betroffenen Person berücksichtigen. Nur wenn das öffentliche Interesse gegenüber dem Schutz der Privatsphäre der betroffenen Person eindeutig überwiegt, dürfen Sie diese Informationen veröffentlichen.

- Das Eingreifen der leitenden Redakteure oder die Hinzuziehung von Sachverständigen kann eine große Hilfe sein, um sicherzustellen, dass diese Anforderung erfüllt wird. Vergessen Sie nicht, dass die interessierten Journalisten in der Regel nicht so objektiv sind, wenn es darum geht, die verschiedenen Interessen abzuwägen.

- Denken Sie immer daran, dass Sie nur Daten sammeln sollten, die für Ihre Untersuchung relevant sind und von öffentlichem Interesse sein könnten. Wenn Sie beispielsweise gegen einen Politiker wegen möglicher Korruptionspraktiken ermitteln und sensible Informationen über seine oder ihre sexuelle Ausrichtung entdecken, sollten Sie diese nicht verarbeiten, sofern sie für die betreffende Angelegenheit nicht relevant sind. Dies ist eine wesentliche Anforderung des Minimierungsprinzips, eines Schlüsselkonzepts der Datenschutz-Grundverordnung.

- In besonders strittigen Fällen, in denen nicht ganz klar ist, ob oder inwieweit die "journalistische Ausnahmeregelung" auf die Datenverarbeitung anwendbar ist, sollte ein Prüfprotokoll geführt werden, um die datenschutzrechtlichen Erwägungen zu erläutern, und die federführende Aufsichtsbehörde sollte um Rat gefragt werden (Biriukova, S. 30).

- Bei der Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie bei der Verarbeitung von genetischen Daten, Daten über die Gesundheit oder Daten über das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder

damit zusammenhängende Sicherheitsmaßnahmen sind besondere Vorsichtsmaßnahmen zu treffen.

- Daten, die schutzbedürftige Personen und insbesondere Minderjährige betreffen, sollten nur verarbeitet werden, wenn triftige Gründe dies rechtfertigen. Sie müssen sich absolut sicher sein, dass sie auf die konkrete Verarbeitung zutreffen, bevor Sie fortfahren.

7. Fragen und Antworten

Wie sieht es mit der Sekundärnutzung von Daten aus?

Die Antwort auf diese Frage hängt von einigen Schlüsselfragen ab. Erstens können Daten, die auf der Grundlage eines berechtigten Interesses, eines Vertrags oder lebenswichtiger Interessen erhoben wurden, für einen anderen Zweck verwendet werden, solange der neue Zweck mit dem ursprünglichen vereinbar ist. Gemäß Artikel 6 Absatz 4 der Datenschutz-Grundverordnung sind dabei unter anderem folgende Punkte zu berücksichtigen

a. jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;
b. den Kontext, in dem die personenbezogenen Daten erhoben wurden, insbesondere im Hinblick auf die Beziehung zwischen den betroffenen Personen und dem für die Verarbeitung Verantwortlichen;
c. die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden;
d. die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
e. das Vorhandensein geeigneter Sicherheitsvorkehrungen, die Verschlüsselung oder Pseudonymisierung umfassen können.

Wenn man die Daten für Statistiken oder wissenschaftliche Forschung verwenden möchte, ist es nicht notwendig, den Kompatibilitätstest durchzuführen. Diese neuen Verwendungszwecke sind gemäß Artikel 5 Absatz 2 Buchstabe b der Datenschutz-Grundverordnung mit dem ursprünglichen Zweck vereinbar.

Wenn man die Daten auf der Grundlage der Einwilligung der betroffenen Personen oder aufgrund einer gesetzlichen Vorschrift verarbeitet, ist keine weitere Verarbeitung möglich, die über das hinausgeht, was durch die ursprüngliche Einwilligung oder die

gesetzlichen Bestimmungen abgedeckt ist. Eine weitere Verarbeitung würde die Einholung einer neuen Einwilligung oder einer neuen Rechtsgrundlage erfordern.

Ich möchte mich auf die Themen konzentrieren, die mit der Kommerzialisierung personenbezogener Daten zu tun haben, und eine wirtschaftliche Bewertung des Umfangs dieses globalen Handelssystems vornehmen.

Im Prinzip ist eine Datenvermarktung nur möglich, wenn keine personenbezogenen Daten betroffen sind. Für den Fall, dass ein Datensatz beide Arten von Daten vermischt, ist die DSGVO anwendbar. Die Kommerzialisierung von Daten wäre also nicht akzeptabel. Personenbezogene Daten sind mit Rechten verbunden. Sie sind keine Waren und können nicht gekauft oder verkauft werden. Weitere Informationen finden Sie in dem Teil der PANELFIT-Leitlinien, der sich mit Datensätzen befasst, und in unserer kritischen Analyse.

Vorratsdatenspeicherung/Speicherung, Recht auf Vergessenwerden

Im Allgemeinen sollten die Daten nicht länger aufbewahrt werden, als für die Zwecke, für die sie erhoben wurden, unbedingt erforderlich ist. Wenn der für die Verarbeitung Verantwortliche der Ansicht ist, dass sie in Zukunft nützlich sein könnten, sollte er diese Auswahl rechtfertigen. In jedem Fall sollten die Daten so gespeichert werden, dass sie den Grundsätzen der Datenminimierung und der Speicherbegrenzung genügen. So sollten sie, wann immer möglich, anonymisiert oder zumindest pseudonymisiert werden.

Das Recht auf Vergessenwerden ist in Artikel 17 der Datenschutz-Grundverordnung geregelt. Wenn die in Artikel 17 Absatz 1 DSGVO genannten Bedingungen erfüllt sind, ist der für die Verarbeitung Verantwortliche "verpflichtet, personenbezogene Daten unverzüglich zu löschen". Allerdings handelt es sich dabei nicht um ein absolutes Recht. In den Ausnahmen des Artikels 17.3 DSGVO werden Fälle genannt, in denen diese Verpflichtung nicht gilt. Eine dieser Bedingungen ist, dass das Recht "nicht gilt, soweit die Verarbeitung (...) für die Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich ist" (Artikel 17 Absatz 3 Buchstabe a). Wie können wir beide Rechte und Interessen - das Recht auf Löschung und das Recht auf freie Meinungsäußerung und Informationsfreiheit - gegeneinander abwägen? Wie der EuGH

in seinem Urteil in der Rechtssache Google 2 erläuterte, ist Artikel 17 Absatz 3 Buchstabe a DSGVO "Ausdruck der Tatsache, dass das Recht auf Schutz personenbezogener Daten kein absolutes Recht ist, sondern (...) im Hinblick auf seine Funktion in der Gesellschaft betrachtet und gemäß dem Grundsatz der Verhältnismäßigkeit gegen andere Grundrechte abgewogen werden muss".[14] Der Gerichtshof "legt ausdrücklich das Erfordernis fest, ein Gleichgewicht zwischen den in den Artikeln 7 und 8 der Charta garantierten Grundrechten auf Privatsphäre und Schutz personenbezogener Daten einerseits und dem in Artikel 11 der Charta garantierten Grundrecht auf Informationsfreiheit andererseits herzustellen".[15] Andererseits wies der EGMR im Urteil "M.L. und W.W. gegen Deutschland" vom 28. Juni 2018 darauf hin, dass die Interessenabwägung kaum zugunsten eines Löschungsantrags gegen den ursprünglichen Verleger ausfallen kann, dessen Tätigkeit im Mittelpunkt dessen steht, was die Meinungsfreiheit schützen soll.[16] Daher gilt das Recht auf Vergessenwerden im Allgemeinen nicht, wenn es die Ausübung des Rechts auf Information behindert.

Datenerhebung bei Ermittlungen, Datenspeicherung, Umgang mit Daten aus vertraulichen Quellen

Das Berufsgeheimnis ist ein grundlegender Wert, der nicht aus Gründen des Datenschutzes gebrochen werden sollte. Höchstwahrscheinlich hat Ihr Mitgliedstaat besondere Vorschriften erlassen, um die Befugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstaben e und f in Bezug auf für die Verarbeitung Verantwortliche oder Auftragsverarbeiter festzulegen, die nach dem Unionsrecht oder dem Recht der Mitgliedstaaten oder nach den von den zuständigen nationalen Stellen erlassenen Vorschriften dem Berufsgeheimnis oder anderen gleichwertigen Geheimhaltungspflichten unterliegen, sofern dies erforderlich und verhältnismäßig ist, um das Recht auf den Schutz personenbezogener Daten mit der Geheimhaltungspflicht in Einklang zu bringen (siehe Artikel 90 der Datenschutz-Grundverordnung). Diese Vorschriften gelten jedoch nur für personenbezogene Daten, die der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter im Rahmen einer Tätigkeit, die der Geheimhaltungspflicht unterliegt, erhalten oder erlangt hat.

14 EuGH, Rechtssache C-136/17, Urteil vom 24. September 2019, Randnr. 57.

15 EuGH, Rechtssache C-136/17, Urteil vom 24. September 2019, Randnr. 59.

16 Europäischer Gerichtshof für Menschenrechte (EGMR), "M.L. und W.W. gegen Deutschland", 28. Juni 2018.

Forensische Forschung/Ermittlungen mit maschinellem Lernen und falsche Ergebnisse solcher Ansätze, die die Bürger betreffen

Journalisten müssen die Richtigkeit ihrer Informationen sorgfältig prüfen. Abgeleitete Daten sind personenbezogene Daten, da sie Informationen über eine identifizierbare Person liefern. Alle in der DSGVO festgelegten Rechte und Pflichten gelten auch für sie.

Spezifische Tools, die die Datenverarbeitung erleichtern können

Das PANELFIT-Handbuch für Journalisten und die Leitlinien könnten für diese Zwecke recht nützlich sein.

Der Lebenszyklus der Datenverarbeitung. Wenn Sie Daten oder z. B. Interviewaufzeichnungen aufbewahren können, wann sollten Sie sie löschen? Bewährte Praktiken für die Unterscheidung zwischen Daten, die unbegrenzt aufbewahrt werden können, und solchen, die gelöscht werden sollten, sowie für die Zeit, die man sich nimmt, um relevante Daten nach einer bestimmten Anzahl von Jahren von den Sicherungsspeichern zu löschen

In der Datenschutz-Grundverordnung gibt es keinen objektiven Standard für eine angemessene Speicherdauer. Es kommt ganz darauf an, ob die Speicherung sinnvoll ist oder nicht. Wenn Sie nachweisen können, dass die Speicherung solcher Daten für den Zweck der Verarbeitung erforderlich ist, können Sie sie auf unbestimmte Zeit aufbewahren. In jedem Fall sollten sie in einer Weise gespeichert werden, die mit den Grundsätzen der Minimierung und Beschränkung der Speicherung vereinbar ist. So sollten sie, wann immer möglich, anonymisiert oder zumindest pseudonymisiert werden.

Verordnung über Gesundheitsinformationen

"Personenbezogene Daten, die aufgrund ihrer Art in Bezug auf die Grundrechte und -freiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da der Kontext ihrer Verarbeitung erhebliche Risiken für die Grundrechte und -freiheiten schaffen könnte" (Erwägungsgrund 51 DSGVO). Daten über die Gesundheit gelten als besondere Kategorien personenbezogener Daten. Gemäß Artikel 9 Absatz 1 dürfen sie nicht verarbeitet werden, es sei denn, es liegt eine Ausnahme vor, die eine solche Verarbeitung zulässt. Die Ausnahmen sind in Artikel 9 Absatz 2 aufgeführt.

Schutz über Bilder

Bilder sind personenbezogene Daten. Daher braucht man eine Rechtsgrundlage für die Verarbeitung solcher Daten. Wenn die Bilder mehreren Personen entsprechen, sollte die Rechtsgrundlage für alle betroffenen Personen gelten. Wenn die Datengrundlage zum Beispiel die Einwilligung ist, sollten Sie die Einwilligung aller Personen haben, die auf dem Foto oder Video abgebildet sind. Natürlich kann das öffentliche Interesse eine hervorragende Rechtsgrundlage für die Verarbeitung sein, aber Sie sollten die Rechte, Freiheiten und Interessen, die auf dem Spiel stehen, sorgfältig abwägen. Wenn Sie z. B. die Identifizierung von Personen vermeiden können, die für die Informationen nicht wesentlich sind, sollten Sie dies tun, insbesondere wenn es sich um Minderjährige handelt.

Wie ist mit Daten umzugehen, die in einem unstrukturierten Format öffentlich zugänglich sind, um einen neuen Datensatz zusammenzustellen, der möglicherweise zu wertvollen Informationen führt, aber auch schutzbedürftigen Personen schadet (z. B. das Abgreifen [öffentlicher] personenbezogener Daten aus sozialen Medien)?

Im Allgemeinen sollten Sie immer eine geeignete Rechtsgrundlage für die Datenverarbeitung finden. Wie bereits erwähnt, ist das berechtigte Interesse in Ermangelung einer Einwilligung die am besten geeignete Grundlage. Wenn es um die schutzbedürftige Bevölkerung geht, sollte dies bei der Abwägung eine wichtige Rolle spielen. Die Verarbeitung wäre nur dann rechtmäßig, wenn das öffentliche Interesse so stark ist, dass es das Interesse der betroffenen Person überwiegt.

Scraping als solches bringt keine Neuerungen in dieser Grundregel. Auch wenn einige Daten öffentlich sind, bedeutet das nicht, dass Sie sie nach Belieben verwenden können. Im Falle von Daten, die in einem sozialen Netzwerk geäußert werden, sollten Sie auch berücksichtigen, dass Sie auch ein Nutzer dieses Netzwerks sind. Die Nutzungsbedingungen gelten also auch für Sie. Dies sollte im Prinzip nicht zu viel bedeuten, aber Sie sollten es im Hinterkopf behalten.

Ausführliche Informationen dazu finden Sie hier:

Moreno Mancosu, Federico Vegetti, What You Can Scrape and *What Is Right to Scrape: A Proposal for a Tool to Collect Public Facebook Data, Social media + Society*, Volume: 6 issue: 3, Article first published online: Juli 31, 2020; Ausgabe veröffentlicht: Juli 1, 2020, unter: https://journals.sagepub.com/doi/full/10.1177/2056305120940703

Wie sollten Sie sich verhalten, wenn Sie eine Pressemitteilung an die berufliche E-Mail-Adresse eines anderen Journalisten senden wollen (vorausgesetzt, Sie hatten vorher keinen Kontakt). Sollten Sie vorher um Erlaubnis bitten (und wie, wenn nicht per E-Mail), oder sollten Sie davon ausgehen, dass der Empfänger ein Interesse daran hat, informiert zu werden, und ihm Ihre Pressemitteilung schicken und ihm die Möglichkeit geben, sich abzumelden? Und was ist mit Folge-E-Mails?

Im Allgemeinen können Sie E-Mails an die beruflichen Adressen von Personen senden, vorausgesetzt, dass:

- Sie haben einen guten Grund zu der Annahme, dass der Empfänger von den in der Pressemitteilung enthaltenen Informationen profitieren kann.
- Sie sollten die Empfänger darüber informieren, welche personenbezogenen Daten Sie verarbeiten, zu welchem Zweck und wie sie ihre Daten aus Ihrer Mailingliste entfernen oder ändern können, falls diese Liste existiert.
- Außerdem sollten Sie die personenbezogenen Daten der Adressaten nicht länger als nötig verarbeiten (z. B. speichern).

Das Versenden von Folgemitteilungen verstößt nicht gegen die Datenschutzgrundverordnung, wenn es die drei in der obigen Antwort beschriebenen Anforderungen erfüllt. Die Datenverarbeitung im Falle einer Folgemeldung sollte denselben Regeln folgen wie bei einer Vorabmeldung.

8. Glossar (Art. 4 GDPR)

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

2. „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das

Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“ jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

6. „Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personen- bezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. „Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

10. „Dritter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

11. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissver- ständlich 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;

12. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

13. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

14. „biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

15. „Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

16. „Hauptniederlassung“

    a) im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

    b) im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsver- arbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

17. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

18. „Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

19. „Unternehmensgruppe“ eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

20. „verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern;

21. „Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

22. „betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

    a) der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,

    b) diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

    c) eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

23. „grenzüberschreitende Verarbeitung“ entweder

    a) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

    b) eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

24. „maßgeblicher und begründeter Einspruch“ einen Einspruch gegen einen Beschlussentwurf im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder ob beabsichtigte Maßnahmen gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

25. „Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([1]);

26. „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Anhang I. Die Abwägungsprüfung

Einleitung: Die Abwägungsprüfung im Zusammenhang mit dem berechtigten Interesse als Rechtsgrundlage für die Verarbeitung

Das berechtigte Interesse ist eine der sechs Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, die in Artikel 6 Absatz 1 der DSGVO aufgeführt sind. Diese Rechtsgrundlage setzt voraus, dass die berechtigten Interessen des für die Verarbeitung Verantwortlichen oder Dritter, an die die Daten weitergegeben werden, gegenüber den Interessen, Grundrechten und Freiheiten der betroffenen Personen überwiegen (Artikel 6 Absatz 1 Buchstabe f). Um zu überprüfen, ob dies tatsächlich der Fall ist, können die für die Verarbeitung Verantwortlichen auf ein Instrument zurückgreifen, das als Abwägungsprüfung bezeichnet wird und z. B. von der Artikel-29-Datenschutzgruppe empfohlen wurde[17]. Mit diesem Instrument soll sichergestellt werden, dass die berechtigten Interessen des für die Verarbeitung Verantwortlichen oder Dritter, an die die Daten weitergegeben werden, Vorrang vor den Interessen und Grundrechten und -freiheiten der betroffenen Personen haben.

Wann haben die Grundrechte und -freiheiten der vom Datenschutz betroffenen Person keinen Vorrang?

Bei der Abwägungsprüfung müssen mehrere Schlüsselfaktoren berücksichtigt werden, die entscheidend dafür sind, welche Interessen, Freiheiten oder Rechte überwiegen, nämlich[18]

- die **Art und Quelle des berechtigten Interesses** - ob die Datenverarbeitung für die Ausübung eines Grundrechts erforderlich ist, anderweitig im öffentlichen Interesse liegt oder in der betreffenden Gemeinschaft anerkannt ist. Eine Bewertung des möglichen Schadens, der dem für die Verarbeitung

17 A29WP, Stellungnahme 06/2014 zum Begriff der berechtigten Interessen des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG. April 2014, S.24. Unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Abgerufen am 05. Januar 2020

18 A29WP, Stellungnahme 06/2014 zum Begriff der berechtigten Interessen des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG. April 2014, S.24. Unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Abgerufen am 05. Januar 2020.

Verantwortlichen, Dritten oder der Allgemeinheit entsteht, wenn die Datenverarbeitung nicht stattfindet, ist obligatorisch.

- Die **Macht und Stellung der beiden Parteien** (für die Verarbeitung Verantwortlicher oder Dritter und betroffene Person). So ist beispielsweise ein Arbeitgeber, der die Daten eines Arbeitnehmers verarbeiten will, in einer stärkeren Position als der Arbeitnehmer. Wenn die betroffene Person minderjährig ist, sollten ihre Interessen, Rechte und Freiheiten überwiegen.

- Die **Art der Daten**. Daten besonderer Kategorien sollten beispielsweise stärker gewichtet werden. Ebenso sollten Daten, die von den Menschen wahrscheinlich als besonders "privat" angesehen werden (z. B. Finanzdaten), Daten von Kindern oder Daten über andere schutzbedürftige Personen angemessen abgewogen werden.

- Die **Auswirkungen der Verarbeitung auf die betroffenen Personen**. Zu diesem Zweck sollten die für die Verarbeitung Verantwortlichen prüfen, ob die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen könnte. Wenn dies der Fall ist, müssen sie eine Datenschutzfolgenabschätzung durchführen.

- **Die berechtigten Erwartungen der** betroffenen Personen, was mit ihren Daten geschehen wird. Die für die Verarbeitung Verantwortlichen sollten in der Lage sein nachzuweisen, dass eine vernünftige Person die Verarbeitung unter den gegebenen Umständen erwarten würde. Wenn der Zweck und die Methode der Verarbeitung nicht sofort ersichtlich sind und die Möglichkeit besteht, dass es eine Reihe von vernünftigen Meinungen darüber gibt, ob die Menschen dies erwarten würden, möchten die für die Verarbeitung Verantwortlichen vielleicht eine Art Konsultation, Fokusgruppe oder Marktforschung mit Einzelpersonen durchführen, um die Erwartungen aufzuzeigen und ihre Position zu unterstützen. Wenn es bereits Studien über angemessene Erwartungen in einem bestimmten Kontext gibt, können sich die für die Verarbeitung Verantwortlichen möglicherweise auf diese stützen, um festzustellen, was Einzelpersonen erwarten können oder nicht[19].

- die **Art und Weise der Datenverarbeitung** (groß angelegter Datenabbau, Profilerstellung, Weitergabe an eine große Zahl von Personen oder Veröffentlichung);

- Die **zusätzlichen Garantien**, die unzumutbare Auswirkungen auf die betroffene Person begrenzen könnten, wie Datenminimierung (z. B. strenge Beschränkung der Datenerhebung oder sofortige Löschung der Daten nach ihrer Verwendung) - technische und organisatorische Maßnahmen, die sicherstellen, dass die Daten nicht für Entscheidungen oder andere Maßnahmen in Bezug auf Einzelpersonen

19 ICO, Wie wenden wir legitime Interessen in der Praxis an? Unter: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Abgerufen am: 15. Januar 2020

verwendet werden können ("funktionale Trennung") - umfassende Verwendung von Anonymisierungstechniken, Datenaggregation, Technologien zum Schutz der Privatsphäre, "Privacy by Design", Folgenabschätzungen zum Schutz der Privatsphäre und des Datenschutzes; erhöhte Transparenz, allgemeines und bedingungsloses Widerspruchsrecht (Opt-out), Datenübertragbarkeit und damit verbundene Maßnahmen zur Stärkung der Rechte der Betroffenen usw.

Die Frage der zusätzlichen Schutzmaßnahmen

Die Artikel-29-Datenschutzgruppe ist der Ansicht, dass Abhilfemaßnahmen und Garantien, wie organisatorische oder technische Maßnahmen, die der für die Verarbeitung Verantwortliche zum Schutz der Rechte der betroffenen Person ergreift, in die Abwägungsprüfung einbezogen werden sollten. Es gibt jedoch einen alternativen Ansatz, demzufolge Artikel 6 Absatz 1 Buchstabe f eine Abwägung zwischen zwei Werten verlangt, nämlich den berechtigten Interessen des für die Verarbeitung Verantwortlichen (oder eines Dritten) und den Interessen, Rechten und Freiheiten der betroffenen Person. Abmilderungsmaßnahmen und Garantien sind mit keinem dieser Werte vereinbar. Sie sollten daher nicht in Betracht gezogen werden. Andernfalls würden sie auf der Seite der für die Verarbeitung Verantwortlichen überwiegen, da sie die Bedeutung des möglichen Schadens für die Interessen, Rechte und Freiheiten der betroffenen Person untergraben würden. Kamara und De Hert haben einige überzeugende Erklärungen zu diesem konkreten Thema abgegeben, indem sie feststellten, dass[20]

> *"Die Einbeziehung von Abhilfemaßnahmen in die Abwägung würde dazu führen, dass die tatsächlich zu erwartenden Auswirkungen der Verarbeitung auf die Rechte der betroffenen Personen dargestellt werden und dass die berechtigten Interessen immer noch überwiegen. Dieser Ansatz "bestraft" nicht den für die Verarbeitung Verantwortlichen, der Abhilfemaßnahmen und Garantien ergreift, indem er sie nicht in die Abwägungsprüfung einbezieht. Im Gegenteil, er ermutigt den für die Verarbeitung Verantwortlichen, dies zu tun. Andererseits ist zu bedenken, dass das Gewicht künftiger Schutz- und Abhilfemaßnahmen immer von ihrer Umsetzung*

20 Kamara, Irene und De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, S.17. Unter: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Zugriff am: 17. Januar 2020

und Wirksamkeit abhängt. Solche Maßnahmen sollten daher in Betracht gezogen werden, aber keine wesentliche Rolle bei der Entscheidung spielen, auf welche Seite sich die Waage neigt.

Einige Beispiele für Abwägungstests

Beispiel 1[21]

Fall: Die Zeitung Z erwägt die Veröffentlichung einiger Fotos, die X, einen Schauspieler, zeigen, nachdem er bei einer öffentlichen Parade wegen Kokainbesitzes verhaftet wurde. X ist in seinem Land eine bekannte Persönlichkeit des öffentlichen Lebens, da er in einer Fernsehserie einen Polizisten spielt. Außerdem hat er mehrere Interviews gegeben, in denen er öffentlich über sein Privatleben Auskunft gegeben hat.

Abwägungsprüfung: Die Daten betreffen eher das Privatleben der Person als das Berufsleben. Die Weitergabe der Daten könnte zu einem erheblichen Schaden für die Person führen. Es besteht jedoch ein öffentliches Interesse an der Weitergabe dieser Informationen. Die Erwartung des Schauspielers, dass seine Privatsphäre wirksam geschützt wird, wurde durch die Tatsache gemindert, dass er in mehreren Interviews Daten aus seinem Privatleben preisgegeben hat. Nach Abwägung aller relevanten Faktoren muss das Unternehmen zu dem Ergebnis kommen, dass die Interessen des berühmten Schauspielers nicht die berechtigten Interessen des Unternehmens an der Veröffentlichung der Fotos überwiegen und die Verarbeitung auf der Grundlage dieser berechtigten Interessen rechtmäßig ist.

Siehe: Axel Springer AG vs. Alemania

Beispiel 2[22]

Der Fall: Ein Arbeitgeber überwacht die Internetnutzung seiner Mitarbeiter während der Arbeitszeit, um sicherzustellen, dass sie die IT des Unternehmens nicht übermäßig privat nutzen. Zu den gesammelten Daten gehören temporäre Dateien und Cookies, die auf den Computern der Beschäftigten erzeugt werden und die während der Arbeitszeit besuchte

21 Quelle: A29WP, Stellungnahme 06/2014 zum Begriff der berechtigten Interessen des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG. April 2014, S.63. Unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Abgerufen am 05. Januar 2020

22 Quelle: ICO. Wie wenden wir legitime Interessen in der Praxis an? Unter: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Zugriff am: 15. Januar 2020

Websites und durchgeführte Downloads aufzeigen. Die Daten werden ohne vorherige Konsultation der betroffenen Personen und der Gewerkschaftsvertreter/des Betriebsrats im Unternehmen verarbeitet. Außerdem werden die betroffenen Personen nicht ausreichend über diese Praktiken informiert.

Abwägungsprüfung: Der Umfang und die Art der erhobenen Daten stellen einen erheblichen Eingriff in das Privatleben der Beschäftigten dar. Neben Fragen der Verhältnismäßigkeit ist auch die Transparenz der Praktiken, die eng mit den berechtigten Erwartungen der betroffenen Personen verknüpft ist, ein wichtiger zu berücksichtigender Faktor. Selbst wenn der Arbeitgeber ein berechtigtes Interesse daran hat, die Zeit zu begrenzen, die die Beschäftigten mit dem Besuch von Websites verbringen, die nicht unmittelbar mit ihrer Arbeit zusammenhängen, erfüllen die angewandten Methoden nicht die Abwägungsprüfung nach Artikel 7 Buchstabe f. Der Arbeitgeber sollte weniger einschneidende Methoden anwenden (z. B. die Einschränkung der Zugänglichkeit bestimmter Websites), die - als bewährte Praxis - mit den Arbeitnehmervertretern erörtert und vereinbart und den Arbeitnehmern auf transparente Weise mitgeteilt werden.

DOs und DON'Ts

Dos

- Überprüfen Sie die Art der verarbeiteten Daten und achten Sie besonders auf den Schutz der Interessen, Rechte und Freiheiten von Kindern, wenn diese gefährdet sind.
- Berücksichtigung der berechtigten Erwartungen der betroffenen Personen
- Durchführung einer DPIA, wenn die Umstände dies empfehlen

DON'Ts

- Verarbeiten Sie die Daten von Kindern nicht, wenn es nicht unbedingt notwendig ist, um das verfolgte Interesse zu erreichen.
- Verarbeiten Sie die Daten nicht, wenn der Abwägungstest nicht schlüssig ist.
- Zögern Sie nicht, angemessene Garantien einzuführen, um die Beeinträchtigung der Interessen, Rechte und Freiheiten der betroffenen Personen zu minimieren.

Checkliste

- Die für die Verarbeitung Verantwortlichen haben sich vergewissert, dass die Interessen des Einzelnen nicht die berechtigten Interessen des für die Verarbeitung Verantwortlichen oder Dritter überwiegen.
- Die für die Verarbeitung Verantwortlichen verwenden die Daten von Personen in einer Weise, die sie vernünftigerweise erwarten können.
- Die für die Verarbeitung Verantwortlichen verwenden die Daten der Personen nicht in einer Weise, die sehr einschneidend ist oder ihnen Schaden zufügen könnte, es sei denn, sie haben einen besonders guten Grund.
- Die für die Verarbeitung Verantwortlichen verarbeiten keine Daten von Kindern, oder wenn sie es doch tun, haben sie besondere Sorgfalt walten lassen, um sicherzustellen, dass ihre Interessen geschützt werden.
- Die Kontrolleure haben Schutzmaßnahmen erwogen, um die Auswirkungen so weit wie möglich zu verringern.
- Die für die Verarbeitung Verantwortlichen haben geprüft, ob sie eine Datenschutzprüfung durchführen müssen.

Weitere Lektüre

- Weitere Beispiele für die Abwägungsprüfung wurden von der Datenschutzbehörde nach Artikel 29 vorgelegt und finden sich in ihrer Stellungnahme 06/2014 zum Begriff der berechtigten Interessen des für die Verarbeitung Verantwortlichen nach Artikel 7 der Richtlinie 95/46/EG

- A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

- EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 april 2017, at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Accessed 5 May 2020

- ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/

- ICO, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Accessed 05 May 2020.

- Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

Anhang II. Vergleichende Analyse des Rechtsrahmens auf der Ebene der EU-Mitgliedstaaten

Die Hauptquelle für die gesammelten Informationen ist die vergleichende Bird&Bird-Analyse, sofern nicht anders angegeben.

Österreich

Zuletzt geprüft am: 05.06.2018

9 ADPA enthält besondere Bestimmungen über die Verarbeitung personenbezogener Daten im Zusammenhang mit der Meinungs- und Informationsfreiheit. Diesen Bestimmungen zufolge gelten mehrere Vorschriften der DSGVO (insbesondere deren Grundsätze und Rechte der betroffenen Personen) nicht für die Verarbeitung personenbezogener Daten für journalistische Zwecke sowie für wissenschaftliche, künstlerische oder literarische Zwecke.

Belgien

Zuletzt geprüft am: 13.09.2018

Abschnitt 16 des DSG erlaubt die Verarbeitung personenbezogener Daten mit angemessenen Mitteln zu journalistischen Zwecken oder zu Zwecken des wissenschaftlichen, künstlerischen oder literarischen Ausdrucks. Die §§ 17 ff. regeln Ausnahmen von der Informationspflicht (§ 17), den Schutz von Quelle und Inhalt der Informationen (§ 18), Ausnahmen vom Recht auf Einschränkung der Verarbeitung (§ 19), Informationen über Berichtigung und Löschung (§ 20) und die Einschränkung des Widerspruchsrechts (§ 21).

Finnland

Zuletzt geprüft am: 13.11.2018

Gemäß Abschnitt 27 des Datenschutzgesetzes gelten nur begrenzte Bestimmungen der Datenschutz-Grundverordnung für die Verarbeitung personenbezogener Daten zum Zwecke des Journalismus oder der wissenschaftlichen, künstlerischen oder literarischen

Darstellung. Mit diesem Ansatz wird die Situation aufrechterhalten, wie sie unter dem aufgehobenen Gesetz über personenbezogene Daten bestand.

Frankreich

Zuletzt geprüft am: 11.02.2019

Wenn personenbezogene Daten zu journalistischen, künstlerischen oder literarischen Zwecken verarbeitet werden, gelten nach dem französischen Rechtsrahmen die Bestimmungen über die Benachrichtigung, die Datenübermittlung, die Rechte der Betroffenen, die Aufbewahrung und die Verarbeitung besonderer Datenkategorien nicht.

Deutschland

Zuletzt überarbeitet am: 23.05.2018

§ 35 des neuen deutschen Bundesdatenschutzgesetzes ("BDSG") befreit den für die Verarbeitung Verantwortlichen von der Verpflichtung zur Löschung personenbezogener Daten, wenn die Löschung im Falle einer nichtautomatisierten Datenverarbeitung unmöglich oder nur mit unverhältnismäßig hohem Aufwand möglich ist und die betroffene Person ein geringes Interesse an der Löschung hat. § 27(2) DSG schränkt die Rechte der Betroffenen unter bestimmten weiteren Voraussetzungen ein.

Irland

Zuletzt geprüft am: 07.06.2018

Gemäß Abschnitt 43(1) des Gesetzes ist die Verarbeitung personenbezogener Daten zum Zweck der Ausübung des Rechts auf freie Meinungsäußerung und Information, einschließlich der Verarbeitung zu journalistischen Zwecken oder zu Zwecken der wissenschaftlichen, künstlerischen oder literarischen Meinungsäußerung, von der Einhaltung bestimmter Vorschriften der Datenschutz-Grundverordnung ausgenommen, wenn die Einhaltung dieser Vorschriften in Anbetracht der Bedeutung des Rechts auf freie Meinungsäußerung und Information in einer demokratischen Gesellschaft mit

diesen Zwecken unvereinbar wäre. Die Datenschutzkommission kann jede Rechtsfrage, bei der zu prüfen ist, ob die Verarbeitung personenbezogener Daten gemäß Abschnitt 43(1) ausgenommen ist, dem High Court zur Entscheidung vorlegen.

Italien.

Zuletzt geprüft am: 25.10.2018

IDPA Titel XII - Abschnitte 136-137-138-139. Der Verhaltenskodex für die Verarbeitung personenbezogener Daten und journalistische Tätigkeiten (Anhang A.1 des IDPA) bleibt in Kraft. Die Vereinbarkeit dieses Kodexes mit der Datenschutz-Grundverordnung wird von der italienischen Datenschutzbehörde (im Folgenden "Behörde") neu bewertet werden. Die Behörde sollte ihn vor Ende des Kalenderjahres überprüfen. Darüber hinaus hat Italien einige Grundsätze für die Freistellung von Journalisten durch einen Ethikkodex aufgenommen, nämlich

a) das Erfordernis, jede Art von Vorzensur zu vermeiden

b) die Ausnahme des Auskunftsrechts bei der Datenerhebung, wenn die Berufsausübung dies erfordert

c) die Pflicht des Journalisten, Fehler und Ungenauigkeiten unverzüglich zu korrigieren

d) die Notwendigkeit, besonders vorsichtig zu sein, wenn die Verarbeitung besonders geschützte Daten betrifft. Unter diesen Umständen ist die Verarbeitung auf Tatsachen von unbestrittenem öffentlichem Interesse zu beschränken. Außerdem ist sie auf die wesentlichen Aspekte der Informationen zu beschränken und es sind Hinweise auf Personen zu vermeiden, die nicht mit ihnen in Verbindung stehen. Auch bei Angelegenheiten, die der Betroffene möglicherweise öffentlich gemacht hat oder die im öffentlichen Verhalten gewürdigt werden, ist das Recht auf Schutz vorbehalten

e) es wird vorgeschlagen, die "Wesentlichkeit" der Informationen zu prüfen, die Verhältnismäßigkeit der Veröffentlichung, so dass sie auf das Wesentliche in Bezug auf den Fall beschränkt wird

f) Bei Nachrichten, die sich auf die Gesundheit beziehen, sind die Würde, der Anstand und das Privatleben der betroffenen Person zu respektieren, insbesondere wenn es sich

um schwere oder tödliche Krankheiten handelt, und es sind keine analytischen Daten oder Daten von rein klinischem Interesse zu veröffentlichen. Von diesem Erfordernis kann jedoch nach dem Grundsatz der Verhältnismäßigkeit abgewichen werden, wenn die betroffene Person eine Position von besonderer öffentlicher Bedeutung innehat. Das Gleiche gilt für Informationen über das Sexualleben.

Die Niederlande

Zuletzt geprüft am: 17.09.2018

Artikel 41 des Ausführungsgesetzes zur DSGVO sieht vor, dass die Ausführungsanordnung zur DSGVO nicht gilt, wenn personenbezogene Daten ausschließlich zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken verarbeitet werden. Darüber hinaus enthält es eine Liste von Kapiteln und Artikeln der DSGVO, die ebenfalls nicht für diese Zwecke gelten: (a) Artikel 7(3), 11(2);(b) Kapitel III; (c) Kapitel IV (mit Ausnahme der Artikel 24, 25, 28, 29 und 32); (d) Kapitel V; (e) Kapitel VI; und (f) Kapitel VII. "Art. 41 UAVG schränkt den Umfang bestimmter Pflichten im Zusammenhang mit (zwingenden) allgemeinen Interessen in Anlehnung an Art. 23 DSGVO ein. Daher sieht er Ausnahmen von den Rechten der betroffenen Person und den Pflichten des für die Verarbeitung Verantwortlichen vor. Die DSGVO gilt teilweise (Art. 12-21 und 34 DSGVO) nicht für die Datenverarbeitung im Hinblick auf - unter anderem - wichtige Ziele des öffentlichen Interesses, der öffentlichen Sicherheit, des Schutzes der betroffenen Person oder der Rechte und Freiheiten anderer Personen und/oder der Beitreibung zivilrechtlicher Forderungen (soweit dies angemessen und verhältnismäßig ist).

Spanien

Zuletzt geprüft am: 05.03.2019

Der SDPA enthält keine Rechtsvorschrift, die das Recht auf freie Meinungsäußerung mit dem Datenschutz in Einklang bringt. Es gibt nur einen Verweis auf die Meinungsfreiheit in Artikel 85 über das Recht auf freie Meinungsäußerung im Internet, das jeder hat.

Schweden

Zuletzt geprüft am: 06.09.2018

Datenschutzgesetz Absatz 1:7: Die DSGVO und das Datenschutzgesetz dürfen nicht angewandt werden, soweit dies gegen die Gesetze zur freien Meinungsäußerung verstoßen würde. Das Datenschutzgesetz sieht vor, dass die Artikel 5-30 und 35-50 der DSGVO nicht auf die Verarbeitung personenbezogener Daten zu journalistischen Zwecken oder zu Zwecken der wissenschaftlichen, künstlerischen oder literarischen Ausdrucksformen anwendbar sind.

Vereinigtes Königreich

Zuletzt überarbeitet am: 23.05.2018

Das Datenschutzgesetz des Vereinigten Königreichs von 2018[23] bietet eine nuanciertere Sicht auf die Grenzen der Ausnahmeregelung und legt nahe, dass einige der Bestimmungen der DSGVO nicht für die Datenverarbeitung gelten, wenn drei kumulative Bedingungen erfüllt sind (Cain, 2018):

- die betreffenden Daten müssen im Hinblick auf die Veröffentlichung von journalistischem Material verarbeitet werden,
- der für die Verarbeitung Verantwortliche muss vernünftigerweise davon ausgehen, dass die Veröffentlichung insbesondere unter Berücksichtigung der besonderen Bedeutung des öffentlichen Interesses an der freien Meinungsäußerung im öffentlichen Interesse liegt, und
- der für die Datenverarbeitung Verantwortliche muss vernünftigerweise davon ausgehen, dass die Anwendung der aufgeführten DSGVO-Bestimmung mit seinem journalistischen Zweck unvereinbar wäre.

Das ICO des Vereinigten Königreichs rät, die zweite Bedingung - "öffentliches Interesse" - von Fall zu Fall zu prüfen und dabei bestehende Verhaltenskodizes zu berücksichtigen und das öffentliche Interesse an dem Thema mit dem Ausmaß des Eingriffs in das Privatleben einer Person abzuwägen. Es ist nicht überraschend, dass das "öffentliche Interesse" als eines der Kriterien aufgenommen wurde, da es in der Rechtsprechung des EGMR eine wichtige Rolle spielt. Obwohl der EGMR darauf verzichtet hat, eine Definition des "öffentlichen Interesses" zu geben, hat er anerkannt, dass dieser Begriff

23 Vid. The UK Data Protection Act 2018, Schedule 2, Part 5, par. 26, http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/5/enacted.

die öffentliche, politische und historische Debatte, Fragen im Zusammenhang mit Politikern, dem Verhalten von Staatsbediensteten, großen Unternehmen, Regierungen und kriminalitätsbezogenen Angelegenheiten umfasst. Allerdings können auch andere, weniger offensichtliche Angelegenheiten als von öffentlichem oder allgemeinem Interesse angesehen werden (Bitiukowa, 21).

Informationen zu Befreiungen und Ausnahmen in Kürze

Die folgende Tabelle (Bitiukowa, 25) enthält einen aktuellen Vergleich zwischen mehreren EU-Mitgliedstaaten hinsichtlich der Regelung der Ausnahmen.

TABLE 3

The scope of the "Journalistic exemption" under the national law of the selected Member States

GDPR Article	Explanation of the Article	Sweden	United Kingdom	Lithuania	Romania
Article 5(1)(f)	Principle of integrity and confidentiality, which means that a data controller (e.g., a media undertaking) must put in place technical and organizational measures to ensure that the personal data it processes is protection from unauthorized disclosure, accidental loss, damage,etc.	Partially exempted[94] ***	Not exempted**	Not exempted	Exempted
Article 6	Lawfulness of processing, which means that each processing operation can only be considered lawful if a data controller can identify a lawful basis for it (consent, contract, public interest, etc.).	Exempted*	Exempted	Not exempted	Exempted
Articles 12-23	Rights of data subjects, meaning that the data controller should provide individuals with information about processing and respond to their requests.	Exempted	Partially exempted[95]	Exempted	Exempted
Article 28	Processor, which means that where a media undertaking outsources data processing to another entity (e.g., a data centre or a data analytics company), they must have a data processing agreement in place with it.	Exempted	Not exempted	Not exempted	Exempted

* **Not exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply with the rule** the content of which is explained in the second column.

** **Exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **does not have to comply with the rule** the content of which is explained in the second column.

*** **Partially exempted** – the controller (a media undertaking, a journalist or another person processing personal data for "journalistic purposes") **has to comply only with the certain aspects of the rule** the content of which is explained in the second column and in the relevant footnote.

Informationsquellen

Literaturverzeichnis

Article 29 Working Party, RECOMMENDATION 1/97 Data protection law and the media. Adopted by the Working Party on 25 February 1997, at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp1_en.pdf. Last visited: 17/10/2020.

BIRD & BIRD, Personal data and freedom of expression, At: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/personal-data-and-freedom-of-expression. Last visited: 17/10/2020.

BENEZIC, Dollores, Romania May Be Using GDPR to Intimidate Journalists, Liberties, 2018, At: https://www.liberties.eu/en/news/politicians-in-romania-use-gdpr-to-intimidate-journalists/16384. Last visited: 17/10/2020.

BITIUKOVA, Natalija, Journalistic exemption under the european data protection law, Vilnius Institute for Policy Analysis, 2020, at: https://vilniusinstitute.lt/wp-content/uploads/2020/01/VIPA_Bitiukova_2020_v4_f.pdf. Last visited: 17/10/2020.

CAIN N. and COWPER-COLES, R., GDPR and the Data Protection Act 2018 – how do they impact publishers?, 25 May 2018, https://www.lexology.com/library/detail.aspx?g=b26433e1-0548-4a9d-8351-f720e737f811. Last visited: 17/10/2020.

CULLAGH K. et al, National adaptations of the GDPR, Luxembourg: Blogdroiteuropéen, 17 February 2019, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf. Last visited: 17/10/2020.

DETREKŐI, Zsuzsa, GDPR in Hungary: A Road to Hell?, At: https://medium.com/center-for-media-data-and-society/gdpr-in-hungary-a-road-to-hell-3b60718a0281. Last visited: 17/10/2020.

DRECHSLER L., The GDPR and Journalism. Protecting Privacy or a Break on Democratic Accountability?, 18 September 2018, https://brusselsprivacyhub.eu/publications/ws21.html. Last visited: 17/10/2020.

ECtHR, Guide on Article 8 of the European Convention on Human Rights, August 2020, at: https://www.echr.coe.int/documents/guide_art_8_eng.pdf. Last visited: 17/10/2020.

EDRI, Proceed with caution, at: https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf. Last visited: 17/10/2020.

NIELSEN, Nikolaj. EU Warns Romania Not to Abuse GDPR Against Press, EU Observer (Nov. 12, 2018

REVENTLOW, Nani Jansen, Symposium on the GDPR and international law. Can the GDPR and freedom of expression coexist? At: https://www.researchgate.net/publication/338407067_Can_the_GDPR_and_Freedom_of_Expression_Coexist. Last visited: 17/10/2020.

The UK Information Commissioner's Office, Data protection and journalism: a guide for the Media, 2014, at: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf. Last visited: 17/10/2020.

WARNER, Bernhard, Online-Privacy Laws Come With a Downside, The Atlantic, 2019, at: https://www.theatlantic.com/ideas/archive/2019/06/europes-gdpr-elevated-privacy-over-press-freedom/590845/. Last visited: 17/10/2020.

Dokumente des Europarates

Convention for the protection of individuals with regard to the processing of personal data

Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership

Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors

Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media

Declaration by the Committee of Ministers on the protection and promotion of investigative journalism (26 September 2007)

Resolution 2066 (2015), Media responsibility and ethics in a changing media environment, Parliamentary Assembly

Resolution 1843 (2011), The protection of privacy and personal data on the Internet and online media, Parliamentary Assembly

Resolution 1165 (1998), Right to privacy, Parliamentary Assembly

Resolution 1003 (1993), Ethics of Journalism, Parliamentary Assembly

Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte

- A v. Norway, No. 28070/06, 9 April 2009
- Ageyev v. Russia, No. 7075/10, 18 April 2013
- Alkaya v. Turkey, No. 42811/06, 9 October 2012
- Armonienė v. Lithuania, No. 36919/02, 25 November 2008
- Axel Springer Ag v. Germany [GC], No. 39954/08, 7 February 2012
- Bédat v. Switzerland [GC], No. 56925/08, 29 March 2016
- Biriuk v. Lithuania, No. 23373/03, 25 November 2008 Björk Eiðsdóttir v. Iceland, No. 46443/09, 10 July 2012
- Bladet Tromsø and Stensaas v. Norway, No. 21980/93, 20 May 1999
- Bodrožić v. Serbia, No. 32550/05, 23 June 2009 Bohlen v. Germany No. 53495/09 and Ernst August von Hannover v. Germany No. 53649/09, 19 February 2015
- Couderc and Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015

- Dorothea Sihler-Jauch against Germany and Günther Jauch v. Germany, Nos. 68273/10 and 34194/11, 24 May 2016 (decision)
- Egeland and Hanseid v. Norway, No. 34438/04, 15 April 2009
- Erla Hlynsdóttir (No.2), No. 54125/10, 21 October 2014
- Feldek v. Slovakia, No. 29032/95, 12 July 2001 Flinkkilä and Others v. Finland, No. 25576/04, 6 April 2010
- Fürst-Pfeifer v. Austria, Nos. 33677/10 and 52340/10, 17 May 2016
- Guseva v. Bulgaria, No. 6987/07, 17 February 2015
- Hachette Filipacchi Associés v. France, No. 71111/01, 14 June 2007
- Hachette Filipacchi Associés v. France [GC], No. 40454/07, 10 November 2015
- Hachette Filipacchi Associés ("Ici Paris") v. France, No. 12268/03, 23 July 2009
- Haldimann and Others v. Switzerland, No. 21830/09, 24 February 2015
- Janowski v. Poland, No. 25716/94, 21 January 1999
- Khan v. Germany, No. 38030/12, 21 September 2016
- Khmel v. Russia, No. 20383/04, 12 December 2012
- Khuzhin and Others v. Russia, No. 13470/02, 23 October 2008
- Krone Verlag GmbH & Co. KG v. Austria, No. 34315/96, 26 February 2002
- Krone Verlag GmbH & Co KG and Krone Multimedia GmbH & Co KG v. Austria, No. 33497/07, 17 January 2012
- Leempoel & S.A. ED. Ciné Revue v. Belgium, No. 64772/01, 9 November 2006
- Lillo-Stenberg and Sæther v. Norway, No. 13258/09, 16 January 2014 Mitkus v. Latvia, No. 7259/03, 2 October 2012
- MGN Limited v. the United Kingdom, No. 39401/04, 18 January 2011
- Mosley v. the United Kingdom, No. 48009/08, 10 May 2011
- Müller v. Germany (Dec.), No. 43829/07, 14 September 2010
- Österreichischer Rundfunk v. Austria, No. 35841/02, 7 December 2006 Guidelines on Safeguarding Privacy in the Media 38
- Peck. V. United Kingdom, No. 44647/98, 28 January 2003 Pentikäinen v. Finland [GC], No. 11882/10, 20 October 2015 Reklos and Davourlis v. Greece, No. 1234/05, 15 January 2009 Renaud v. France, No. 13290/07, 25 February 2010
- Salihu and Others v. Sweden, No. 33628/15, 10 May 2016 (decision)
- Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland, No. 34124/06, 21 June 2012

- Selistö v. Finland, No. 56767/00, 16 November 2004
- Standard Verlags GmbH v. Austria (No.2), No. 21277/05, 4 June 2009
- Standard Verlags GmbH v. Austria (No. 3), No. 34702/07, 10 January 2012
- Toma v. Romania, No. 42716/02, 24 February 2009
- Verlagsgruppe News GmbH v. Austria, No. 10520/02, 14 December 2006
- Von Hannover v. Germany, No. 59320/00, 24 June 2004
- Von Hannover v. Germany (No.2) [GC], Nos. 40660/08 and 60641/08, 7 February 2012
- White v. Sweden, No. 42435/02, 19 September 2006
- Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no.2), No. 62746/00, 14 November 2002 (decision)
- Y v. Switzerland, No. 22998/13, 06 June 2017
- Zvagulis v. Lithuania, No. 8619/09, 26 January 2017 (decision)