WDR

15/16

BERICHT DER DATENSCHUTZ BEAUFTRAGTEN

2015/2016

24. BERICHT DER DATENSCHUTZBEAUFTRAGTEN 2015/2016

Inhaltsverzeichnis

Das Thema

Das Thema Datenschutz betrifft uns alle, egal ob online, bei der täglichen Arbeit mit dem PC oder im Zusammenhang mit der Nutzung von mobilen Endgeräten. Stets und ständig werden personenbezogene Daten nutzbar gemacht. Datenschutz wird immer wichtiger, komplexer und nicht zuletzt durch Snowden, NSA, Google und Facebook populärer. Auf der einen Seite sind wir alle vermeintlich sensibler geworden, was das Thema Datenschutz angeht. Auf der anderen Seite verleitet der Service des technischen Fortschritts viele Menschen dazu, gedankenlos von sich aus unzählige Informationen preiszugeben, ohne sich wirklich dafür zu interessieren, wie diese Informationen wirtschaftlich ausgewertet werden können. Der Imageverlust, den ein Datenschutzskandal verursachen kann, ist immens.

Die immer schneller voranschreitende technische Entwicklung zwingt den Gesetzgeber, bei datenschutzrechtlichen Vorgaben allgemein zu bleiben und schafft damit Ermessensspielräume. Um nachhaltige und wirtschaftliche Entscheidungen treffen zu können, müssen Entscheider nicht nur die aktuelle Rechtslage kennen, sondern auch politisch erahnen, welche Entwicklungen anstehen. Auch ein technisches Verständnis ist für eine effektive Beurteilung datenschutzrechtlicher Sachverhalte erforderlich.

Die Aufgabe

Innerhalb des WDR ist es Aufgabe der Datenschutzbeauftragten, bei der Gestaltung und Auswahl oder der Änderung von Verfahren zur Verarbeitung personenbezogener Daten zu beraten.

Mit meiner Bestellung zum 1. August 2016 bin ich die erste Datenschutzbeauftragte im WDR, die sich dieser Aufgabe ausschließlich und in Vollzeit widmet. So sieht es das novellierte WDR-Gesetz vor. Diese gesetzgeberische Chance zur Professionalisierung des Datenschutzes möchte ich nutzen und die Herausforderung annehmen, Qualität und Prestige des Datenschutzes zu verbessern und den digitalen Wandel im WDR effizient zu begleiten und voran zu bringen. Datenschutz muss einen Mehrwert durch Service bieten, beraten, bei Verhandlungen unterstützen, datenschutzkonforme Varianten und Alternativen aufzeigen. Auf der anderen Seite müssen Schäden durch Datenschutz-Skandale unbedingt abgewendet werden. Nur durch vertrauensvolle Zusammenarbeit können wir gemeinsam datenschutzkonform und innovativ Gestaltungsfreiheiten nutzen.

Neben meiner Beratungsfunktion obliegt mir nach § 53 Absatz 1 WDR-Gesetz die unabhängige und vor allem staatsferne datenschutzrechtliche Aufsicht über den WDR. Diese ist Ausfluss des Grundrechts der Rundfunkfreiheit aus Artikel 5 Absatz 1 Satz 2 Alternative 2 GG.

Entsprechend § 53 Absatz 7 WDR-Gesetz erstatte ich hiermit dem Rundfunkrat Tätigkeitsbericht. Der Bericht bezieht sich auf den Zeitraum 1. Januar 2015 bis 31. Dezember 2016. Dies betrifft für die Zeit bis zum 31. Juli 2016 die Tätigkeit meiner Vorgängerin, Beate Ritter, die die Aufgabe neben ihrer Funktion als Abteilungsleiterin im Hörfunk wahrgenommen hat. Um Wiederholungen zu vermeiden, konzentriert sich dieser Bericht weitgehend auf nach Februar 2016 (Stand des 23. Tätigkeitsberichts) ausgeführte Tätigkeiten.

Im Berichtszeitraum gab es weder seitens meiner Vorgängerin noch meinerseits Anlass für förmliche Beanstandungen im Sinne von § 53 Absatz 3 WDR-Gesetz.

Danken möchte ich der Geschäftsstelle des Verwaltungsrates als Vertreterin meiner Dienstaufsicht, Roland Boysen, Justiziariat, Norbert Gust, IT-Sicherheitsbeauftragter, Peter Ladwig, Netze und Security, sowie Kerstin Arens und Christian Kruse, Datenschutzreferat des Zentralen Beitragsservice, und allen übrigen Mitgliedern des Arbeitskreises der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) für die stets kompetente, engagierte und kollegiale Zusammenarbeit. Auch danken möchte ich Petra Baumann, die das Datenschutzreferat 22 Jahre lang unterstützt hat. Besonders danken möchte ich meinem Stellvertreter, Günter Grießbach, für die kompetente Einarbeitung und kontinuierliche Unterstützung.

Köln, im Mai 2017 Karin Wagner

1. EU-Datenschutzgrund-verordnung

Im Folgenden soll ein kurzer Überblick gegeben werden, wie sich das Datenschutzrecht im Berichtszeitraum entwickelt hat und welche Auswirkungen dies konkret für den WDR hat.

Besonders bedeutsam für meine Tätigkeit als Datenschutzbeauftragte in Europa ist die Datenschutz-Grundverordnung (DS-GVO), die am 25. Mai 2016 in Kraft getreten ist, aber erst nach einer zweijährigen Übergangsphase gelten wird. Sie wird ab dem 25. Mai 2018 Wirkung entfalten und die seit 1995 geltende EU-Datenschutzrichtlinie ersetzen. Als *Verordnung* gilt sie unmittelbar in jedem Mitgliedstaat. Als *Grundverordnung* sieht sie zahlreiche Öffnungsklauseln vor, die den mitgliedstaatlichen Gesetzgebern Gestaltungsmöglichkeiten eröffnen und Regelungsaufträge erteilen.

Für Medienunternehmen wie den WDR ist hier insbesondere Artikel 85 Absatz 1 und 2 der DS-GVO von Interesse. Danach bringen die Mitgliedstaaten „durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken und zu wissenschaftlichen, künstlerischen oder literarischen Zwecken in Einklang“. Mit anderen Worten: Der nationale Gesetzgeber ist in der Verantwortung die widerstreitenden Interessen von Medienfreiheit auf der einen Seite und dem Recht auf Datenschutz auf der anderen Seite zum Ausgleich zu bringen. Damit hat der europäische Verordnungsgeber die Notwendigkeit von Ausnahmeregelungen und Einschränkungen in Bezug auf den Datenschutz in den Medien anerkannt und die in Deutschland bereits bestehenden Regelungen zum sogenannten „Medienprivileg“ dem Grunde nach bestätigt und damit deren grundsätzliche Fortgeltung ermöglicht. Außerdem hat er in Erwägungsgrund 153 letzter Satz zur DS-GVO eine weite Auslegung des Begriffs Journalismus gefordert, um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen.

1.1. Medienprivileg

1.1.1. Was bedeutet Medienprivileg?

Hintergrund des Medienprivilegs ist allgemein die Sicherung der in Artikel 5 Absatz 1 Satz 2 GG gewährleisteten Presse- und Rundfunkfreiheit gegenüber dem Staat. Den öffentlich-rechtlichen Rundfunkanstalten kommt dadurch eine besondere Stellung in der deutschen Verfassungsordnung zu. Das Medienprivileg folgt aus einer Abwägung zwischen dem Interesse einer Person am Schutz ihrer personenbezogenen Daten und der Bedeutung der Rundfunkfreiheit für ein pluralistisches Gemeinwesen. Im Hinblick auf das Datenschutzrecht hat dies Auswirkungen auf den Geltungsumfang des Datenschutzrechts im Bereich des Rundfunks.

Das Medienprivileg ist bislang für den WDR in § 49 WDR-Gesetz geregelt. Danach finden die Bestimmungen über den Datenschutz auf personenbezogene Daten, die ausschließlich eigenen journalistisch-publizistischen Zwecken des WDR dienen, nur eingeschränkt Anwendung. Soweit das Medienprivileg reicht, gilt die Einschränkung, dass nur für die Datensicherung maßgebliche Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen Anwendung finden. Das sogenannte datenschutzrechtliche Verbot mit Erlaubnisvorbehalt greift jedoch nicht. Was heißt das? Gäbe es diese Ausnahme nicht, wäre eine Verarbeitung personenbezogener Daten grundsätzlich verboten, es sei denn, eine Rechtsvorschrift erlaubte sie oder es läge eine diesbezügliche Einwilligung des Betroffenen vor. Könnten Journalistinnen und Journalisten[1] personenbezogene Daten nur dann verarbeiten, wenn ein Gesetz dies gestattet oder die Betroffenen einwilligen, wäre die journalistische Tätigkeit massiv eingeschränkt. Freier und kritischer Journalismus als Kernelement der Rundfunkfreiheit und damit auch der demokratischen Grundordnung, wäre faktisch nicht möglich.

1.1.2. Anpassungsbedarf der Landesgesetze

Zur Sicherung dieses Medienprivilegs im Sinne von Artikel 85 Absatz 2 DS-GVO besteht also kein materieller Regelungsbedarf. Die landesrechtlichen Regelungen müssen lediglich statt bisher auf die landesgesetzlichen Regelungen, auf die Regelungen der DS-GVO Bezug nehmen und entsprechend des Medienprivilegs den

[1] Zur besseren Lesbarkeit wird im Folgenden ausschließlich eine Bezeichnungsform verwendet. Selbstverständlich sind alle Formulierungen für alle Geschlechter gleichermaßen zutreffend.

Datenschutz bei einer Datenverarbeitung zu journalistischen Zwecken auf die Regeln zur Datensicherheit und Datenvertraulichkeit im Sinne von Artikel 24 und 32 DS-GVO beschränken.

Der Ausgleich zwischen dem Persönlichkeitsrecht der Betroffenen und der Recherchefreiheit der Journalisten erfolgt über zivil- und strafrechtliche Vorschriften, die dem Betroffenen vielfältige Ansprüche für den Fall der rechtswidrigen Erfassung und Darstellung seiner Person zur Seite stellen.

1.1.3. Datenschutzaufsicht über den WDR

Weiterer Ausfluss des Medienprivilegs ist der Grundsatz der sogenannten Staatsferne für den öffentlich-rechtlichen Rundfunk. Aufgrund der besonderen Bedeutung der Rundfunkfreiheit für die demokratische Willensbildung müssen staatliche Ausforschungen und Einflussnahmen verhindert werden. Aus diesem Grund wird die Datenschutzaufsicht im öffentlich-rechtlichen Rundfunk besonders geregelt.

Nach § 53 Absatz 1 Satz 1 WDR-Gesetz tritt der/die Beauftragte für den Datenschutz beim WDR an die Stelle des oder der Landesbeauftragten für den Datenschutz und Informationsfreiheit. Für den Westdeutschen Rundfunk wurde diese Aufsichtsfunktion mit der Novellierung des WDR-Gesetzes am 27. Januar 2016 weiter gestärkt. Die Novellierung schreibt eine Hauptamtlichkeit des/der Datenschutzbeauftragten vor. In § 53 Absatz 2 Satz 2 WDR-Gesetz heißt es insoweit: „Sie oder er darf während dieser Tätigkeit keine weiteren Aufgaben innerhalb der Anstalt übernehmen.“ Mit der Hauptamtlichkeit des/der Datenschutzbeauftragten des WDR geht dadurch eine weitere Stärkung der Unabhängigkeit des Amts und der damit verbundenen Aufsichtsfunktion einher.

Grundsätzlich ist insoweit von einer Vereinbarkeit der geltenden Regelungen zur Datenschutzaufsicht mit den Vorgaben der DS-GVO auszugehen. So sieht die DS-GVO insbesondere vor, dass in einem Mitgliedstaat mehrere unabhängige Aufsichtsbehörden für die Überwachung der Anwendung der DS-GVO zuständig sein können.

1.2. Konkreter Umsetzungsbedarf im WDR

Um den WDR bestmöglich bei der Umsetzung der Vorgaben der DS-GVO unterstützen zu können, habe ich mich einer Unterarbeitsgruppe des AK DSB zur Umsetzung der DS-GVO angeschlossen, die sich intensiv mit den praktischen Auswirkungen der DS-GVO auf die Häuser beschäftigt.

1.2.1. Themen

Als Themen identifizieren wir zunächst:

\ Artikel 5 Absatz 2 DS-GVO: Dokumentation und Nachweise/ „Rechenschaftspflicht“
\ Artikel 13, 14, 15 DS-GVO: Umsetzung von Transparenzanforderungen/ Auskunftsrechte der Betroffenen
\ Artikel 35 DS-GVO: Datenschutz-Folgenabschätzung
\ Artikel 28 DS-GVO: Anpassungserfordernisse in Bezug auf Auftragsverarbeitungen
\ Anpassungserfordernisse bei Online- und Telemedien
\ IT-Sicherheit gemäß Artikel 32 DS-GVO bzw. Sicherheit der Verarbeitung

WDR-seitig haben wir uns in diesem Zusammenhang mit den Themen Datenschutz-Folgenabschätzung (DSFA) sowie IT-Sicherheit gemäß Artikel 32 DS-GVO beschäftigt, die ich im Folgenden kurz vorstellen möchte:

1.2.2. Datenschutz-Folgenabschätzung (DSFA)

Die Pflicht zur datenschutzrechtlichen Risikofolgenabschätzung trifft die verantwortliche Stelle, also die jeweiligen Fachbereiche. Sie müssen sämtliche in ihren Verantwortungsbereich fallenden Verfahren in Bezug auf ein hohes Datenschutzverletzungsrisiko bewerten und diese Evaluation dokumentieren. Wenn eine Risikoanalyse im Bestand erfolgt ist, sollte ein Prozess aufgesetzt werden, wie in Zukunft vor Beginn einer Verarbeitungstätigkeit routinemäßig geprüft wird, ob eine DSFA durchzuführen ist. Bei mehreren ähnlichen Verarbeitungsvorgängen mit ähnlich hohen Risiken kann grundsätzlich eine einheitliche Abschätzung erfolgen. Artikel 35 Absatz 3 DS-GVO nennt gesetzliche Regelbeispiele für ein Prüfungserfordernis.[2] Nach Artikel 35 Absatz 4 und 5 DS-GVO wird es außerdem „Black-

[2] Zum Beispiel Profiling; umfangreiche Verarbeitung besonderer personenbezogener Daten (wie rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, genetische/biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung); Daten über strafrechtliche Verurteilungen und Straftaten; systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

bzw. Whitelists der Datenschutzaufsicht“ geben, wann eine DSFA durchzuführen ist.

In Artikel 35 Absatz 7 DS-GVO finden sich die inhaltlichen Mindestanforderungen an eine DSFA. So muss eine DSFA eine systematische Beschreibung der Verarbeitungsvorgänge und Zwecke der Verarbeitung enthalten. Die berechtigten Interessen des Verantwortlichen sind zu beschreiben sowie die Verhältnismäßigkeit und Notwendigkeit der Verarbeitung festzulegen. Zusätzlich ist eine systematische Risikobeurteilung durchzuführen. Durch geeignete Maßnahmen wird das Risiko minimiert. Wird das Restrisiko nach Durchführung der Maßnahme noch als hoch eingeschätzt, ist die zuständige Aufsichtsbehörde zu konsultieren, Artikel 36 DS-GVO (dazu im Folgenden mehr).

Grundsätzlich handelt es sich bei der DSFA um eine Art Risikoanalyse. Risiken werden dabei grundsätzlich bewertet, indem ein zu erwartender Schaden in Relation zu der diesbezüglich erwarteten Eintrittswahrscheinlichkeit gesetzt wird. Risikomanagement ist insoweit Managementaufgabe, als es nicht darum geht, Datenschutzschäden per se auszuschließen, was schlicht nicht möglich wäre, sondern diese Risiken transparent zu machen und sie zu steuern. Es sollte also zunächst geprüft werden, ob die bestehenden Risikomanagement-Systeme in den einzelnen Häusern sich eigenen, um mit der DSFA auf ihnen aufzubauen.

Wir als Datenschutzbeauftragte stehen in der Anfangsphase beratend zur Seite. Nach DS-GVO ist es außerdem unsere Aufgabe, die Funktionsfähigkeit der Prozesse zu überwachen. Zu der Kernberatungstätigkeit dürfte zunächst gehören, verschiedene datenschutzrechtliche Schadenskategorien mit den Entscheidern der einzelnen Häuser zu identifizieren. Es wird sich im Zweifel nicht um monetäre Risikokategorien, sondern um Abstufungen im Hinblick auf Imageschäden handeln. Die DS-GVO gibt hier aber bereits selbst eine Hilfestellung in Erwägungsgrund 75 bei der Kategorisierung. So sind bei datenschutzrechtlichen Risikokategorien insbesondere zu denken an Diskriminierung, Identitätsdiebstahl, finanziellen Verlust, Rufschädigung, Hinderung bei der Kontrolle über eigene Daten und Profilbildung mit Standortdaten.

Bei identifiziertem erhöhtem Risiko der Verletzung von Datenschutzrechten Einzelner ist die Aufsichtsbehörde, bin also beim WDR ich, einzuschalten, wenn nach der DSFA trotz Abhilfemaßnahmen ein hohes Risiko verbleibt, Artikel 36 Absatz 1 DS-GVO.

1.2.3. IT-Sicherheit gemäß Artikel 32 DS-GVO

Als weiteres Thema haben wir uns um die technisch-organisatorischen Maßnahmen, unter Datenschützern kurz liebevoll TOMs nach Art 32 DS-GVO und den diesbezüglichen Anpassungsbedarf gekümmert.

Die bisherigen TOMs müssen gesichtet und auf die neuen „Kategorien“ angepasst/übersetzt werden. Kurz zusammengefasst kategorisieren sich die neuen TOMs nach DS-GVO wie folgt: a) Pseudonymisierung und Verschlüsselung; b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit; c) Wiederherstellbarkeit.

Die Anpassungsverantwortlichkeit trifft auch hier wieder die verantwortliche Stelle, aber auch den Auftragsdatenverarbeiter, der nach DS-GVO nun Auftragsverarbeiter heißt.

Um das Rad nicht neu erfinden zu müssen und alte Verfahrensverzeichnisse und Anlagen von Auftragsdatenverarbeitungsverträgen ganz erneuern zu müssen, sollte überlegt werden, wie man effektiv die bestehenden TOMs in die Anforderungen und Kategorien der DS-GVO überführen kann.

Gänzlich neu ist Punkt d), wonach ein Verfahren zu etablieren ist, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht. Bei der Implementierung dieses risikobasierten Ansatzes zur Evaluierung von TOMs, sollte man sich an dem ebenfalls risikobasierten Ansatz der DSFA orientieren.

2. Auftragsdatenverarbeitung (ADV)

Ein Hauptaufgabenfeld bei meiner Tätigkeit als Datenschutzbeauftragte liegt in der Überprüfung von ADV-Verhältnissen. Nach § 11 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) bleibt der Auftraggeber bei einer ADV für die Einhaltung der Vorschriften über den Datenschutz verantwortlich. Der Auftragnehmer wird -rein weisungsgebunden- als verlängerter Arm des Auftraggebers tätig, ohne eigene Entscheidungsbefugnis oder eigenes Interesse an der Datenverarbeitung. Damit müssen wir als Auftraggeber bei der Auswahl von Auftragnehmern besonders sorgfältig sein und diese in datenschutzrechtlicher Hinsicht vorab und fortlaufend überprüfen. Diese Prüfpflicht wirkt bis in etwaige Unterauftragsverhältnisse weiter. Dafür wird die Auftragsdatenverarbeitung gemäß § 3 Absatz 4 DSG NRW privilegiert. Das heißt, dass es für eine Datenübermittlung an den Auftragnehmer keiner gesonderten Rechtsgrundlage bedarf, sofern er die personenbezogenen Daten im Geltungsbereich der Datenschutzvorschriften der Europäischen Union verarbeitet.

2.1. Datenübermittlung in das außereuropäische Ausland

Bei einer Datenübermittlung in das außereuropäische Ausland sollten bereits jetzt die Grundsätze der Artikel 44 ff. DS-GVO eingehalten werden. Danach ist eine solche Datenübermittlung nur zulässig, wenn das Drittland, in das die Daten übermittelt werden sollen, ein der DS-GVO entsprechendes Schutzniveau gewährleistet.

2.1.1. Angemessenheitsbeschluss im Sinne von Art 45 DS-GVO

Nach Artikel 45 DS-GVO kann das Schutzniveau durch einen Angemessenheitsbeschluss der Kommission gewährleistet werden. Diese Beschlüsse haben allerdings nur eine Gültigkeitsdauer von maximal vier Jahren, nach denen eine erneute Prüfung durch die Kommission erfolgen muss. Der Europäische Gerichtshof hat am 6. Oktober 2015 das Safe-Harbor-Abkommen zwischen den USA und der EU für ungültig erklärt, wodurch alle auf Safe-Harbor basierenden transatlantischen Datenübermittlungen nachträglich ihre Rechtmäßigkeit verloren.

Am 2. Februar 2016 haben die EU und die USA sich auf ein Nachfolge-Abkommen zu Safe-Harbor geeinigt, das sogenannte „Privacy Shield“. Trotz harscher Kritik aus Datenschützer-Kreisen hat die EU-Kommission am 12. Juli 2016 beschlossen, dass dieses Datenschutzabkommen dem Datenschutzniveau der Europäischen Union entspreche, was einem Angemessenheitsbeschluss im Sinne von Artikel 45 DS-GVO gleich kommt. Es ist allerdings fraglich, ob das Abkommen einer gerichtlichen Prüfung durch den EuGH standhalten wird oder ein ähnliches Schicksal erleidet, wie sein Vorgänger.

2.1.2. Geeignete Garantien i.S.v. Artikel 46 DS-GVO

Nach Artikel 46 DS-GVO können aber auch geeignete Garantien eine Datenübermittlung in das EU-Ausland rechtfertigen. Eine solch geeignete Garantie stellen die sogenannten EU-Standardvertragsklauseln dar. Im Gegensatz zu den unter einen Angemessenheitsbeschluss fallenden Abkommen zwischen Staaten und Staatengemeinschaften, handelt es sich hierbei um eine Art Allgemeine Geschäftsbedingung (AGB), die zwischen den Vertragsparteien abgeschlossen werden. Sie legen zwischen den Parteien vertraglich fest, was unter den Anwendungsbereich der DS-GVO fallende Vertragspartner bereits gesetzlich zu befolgen haben. Dadurch unterliegen die Garantien auch keinem Verfallsdatum, wie die Angemessenheitsbeschlüsse.

Aus diesem Grund empfehlen wir für den WDR die Nutzung der sogenannten EU-Standardvertragsklauseln, falls sich eine Datenübermittlung in das außereuropäische Ausland nicht vermeiden lässt.

2.2. ADV-Vereinbarung

Innereuropäisch ist die Vertragsgestaltung ein wenig einfacher, doch auch hier ein schriftlicher ADV-Vertrag zwingend notwendig. Auftragnehmer, auf die das DSG NRW und auch das WDR-Gesetz per se keine Anwendung finden, müssen auf die entsprechenden für den WDR geltenden Gesetze verpflichtet und insbesondere meiner Aufsicht als insoweit zuständiger Landesbeauftragter für Datenschutz und Informationsfreiheit unterworfen werden. Bei jeder Auftragsdatenverarbeitung muss deshalb der jeweilige Auftragnehmer eine Auftragsdatenverarbeitungsvereinbarung -im WDR als „Sicherheitsvereinbarung“ bezeichnete AGB -unterzeichnen. Diese „Sicherheitsvereinbarung“ wurde Ende 2016 angepasst und wird bis zum Wirksamwerden der DS-GVO durch ein auf Art 28 DS-GVO Bezug nehmendes Papier zu ersetzen sein.

2.3. Beispiel Konditionsrahmenvertrag: Streaming-Kapazitäten

„UEFA EURO 2016

sportschau.de mit Millionenabrufen am ersten ARD-Tag

Der erste ARD-Tag bei der EURO 2016 mit dem deutschen Spiel gegen die Ukraine stößt auch bei sportschau.de auf viel Resonanz: Das Onlineangebot der Sportschau inklusive der Sportschau-App wurde am 12. Juni insgesamt mehr als zwei Millionen Mal besucht und verzeichnete 6,9 Millionen. Page Impressions. Dazu kommen über den Tag verteilt rund 1,6 Mio. Aufrufe für den Livestream der Sportschau. Auch der Livestream bei dasErste.de wurde mit 1,95 Mio. Zugriffen über den gesamten Tag weit über dem Durchschnitt abgerufen. Stark nachgefragt wurde vor allem das neue Multicam-Angebot der Sportschau, bei dem man Livestreams und Highlight-Videos aus verschiedenen Kameraperspektiven betrachten kann: Allein am 12. Juni wurden mehr als 350 000 Videoabrufe gezählt.“

Streaming-Dienstleister, die eine solch hohe Auslastung zuverlässig gewährleisten, sind nicht im Anwendungsbereich des Europäischen Datenschutzrechts beheimatet. Dieses Problems musste ich gleich zu Beginn meiner Tätigkeit als einer meiner ersten Amtshandlungen Herr werden. Bei der Verhandlung bzw. Begleitung der EU-weiten Ausschreibung für einen Konditionsrahmenvertrag bezüglich Streaming-Kapazitäten für die ARD und das ZDF hatte der WDR die Federführung inne.

Grundsätzliche Vorgabe aus dem Kreis der Datenschutzbeauftragten, die ich in diesem Zusammenhang zu vertreten hatte, war der Verbleib aller personenbezogenen Daten (also insbesondere klarsprechender IP-Adressen) im Europäischen Wirtschaftsraum (EWR).

Da es keine potenziellen Anbieter mit Hauptsitz im EWR gab, war diese Vorgabe in wirtschaftlicher Hinsicht nicht ohne Einschränkungen umsetzbar. Die verhandelnden Kollegen der Auftragskoordination hatten bei meinem Einstieg bereits erreicht, dass die Anbieter zu einer Verlagerung von Serverstandorten in die EU bereit waren, ohne dass eine Kostenabwälzung für diese Verlagerung auf den öffentlich-rechtlichen Rundfunk stattfinden würde. Dies ist insoweit als positives Zeichen aus Sicht des Datenschutzes zu werten, als sich damit ein weiteres Geschäftsfeld, das ausschließlich aus dem nicht europäischen Bereich angeboten wird, bereit macht für den europäischen Markt mit seinen datenschutzrechtlichen Vorgaben.

Dieses Entgegenkommen änderte jedoch nichts an der Tatsache, dass gewisse Einschränkungen dennoch gemacht werden mussten, weil eine Störungsbeseitigung für gewisse Notfälle nur vom Hauptsitz aus möglich blieb. Für diese Fälle erarbeiteten die Kollegen der Programmverbreitung einen abschließenden Ausnahmekatalog zur Sicherstellung der Service-Qualität sowie zur Störungsbeseitigung:

„1. Zur Aufrechterhaltung der Service-Qualität des CDN[3]s dürfen IP-Adressen in dringenden Ausnahmefällen (zum Beispiel DDos-Attacken, Routing-Optimierungen, Transit-/Peering-Störungen) in Drittländer transferiert werden. In diesem Fall muss der Auftragnehmer den Auftraggeber unverzüglich in folgender Struktur informieren: IP-Adresse, Grund der Maßnahme und Adressat (Organisationseinheit) der Übermittlung, Standort der Organisationseinheit und Zeitpunkt der Übermittlung.

2. Klarsprechende IP-Adressen dürfen auch dann in Drittländer transferiert werden, wenn der Auftraggeber an den Auftragnehmer Störungen der Verfügbarkeit der Dienste bei End-Usern meldet. In solchen Fällen erteilen die End-User gegenüber dem Auftraggeber ihre explizite Einwilligung in die Übermittlung des Drittlandes.“

Nach Abschluss der jeweiligen Einzel-Maßnahmen ist der WDR automatisch zu informieren und alle klarsprechenden IP-Adressen sind spätestens nach 14 Tagen ohne unsere explizite Aufforderung zu löschen oder zu anonymisieren.

Außerdem erhält der WDR über die vorgenannten Ausnahmefälle quartalsmäßig ein konsolidiertes Reporting in auswertbarer Form, das den Löschvorgang mit Datum und durchführender Stelle dokumentiert.

Voraussetzung für eine Zulässigkeit der Datenübermittlung ins EU-Ausland war darüber hinaus gemäß

[3] CDN = Content Delivery Network

§ 17 DSG NRW die Gewährleistung eines angemessenen Datenschutzniveaus der empfangenden Stelle. Dieses wurde im vorliegenden Fall durch die Einbeziehung von Standardvertragsklauseln gewährleistet.

2.4. Cloud Computing

Auch das derzeit allgegenwärtige Thema „Cloud“ ist datenschutzrechtlich in der Regel nichts anderes als eine Auftragsdatenverarbeitung.

2.4.1. Was ist „Cloud Computing“?[4]

Durch die weltweite Vernetzung und die damit verbundene Datenübermittlung benötigen Unternehmen für ihre bestehenden Systeme immer mehr Leistungen (Rechenleistung, Speicher, Performance etc.). Wenn jedes Unternehmen, die für ihre computerisierten Arbeitsabläufe auch in Spitzenzeiten notwendige Rechenleistung im eigenen Haus unterhalten würde, wäre das ein gewaltiger Aufwand. D.h. dafür wären zusätzliche zahlreiche Server, die auch gewartet und regelmäßig erneuert werden müssten, notwendig. An dieser Stelle entstand die Nachfrage nach entsprechenden Dienstleistungen aus dem Netz, die heute unter dem Begriff Cloud Computing zusammengefasst werden.

Leistungen aus der „WOLKE“. Einfach ausgedrückt handelt es sich dabei um das Outsourcen von Soft- oder Hardware ins Internet zu einem externen Cloud Computing Anbieter.

Kostenersparnis und hohe Flexibilität machen Cloud-Dienste attraktiv für Unternehmen. Software muss nicht auf dem eigenen Computer laufen, Daten werden nicht auf der lokalen Festplatte gespeichert. Der Zugriff auf die Daten ist von überall möglich, weil sie im Netz bei dem gewählten Cloud-Dienstleister liegen. Man muss keine neuen Ressourcen wie zum Beispiel Festplatten und Server kaufen. Wenn man mehr Leistung braucht, mietet man einfach welche hinzu.

So attraktiv das Konzept auch ist, wirft Cloud Computing auch Fragen auf und hat auch Nachteile, die nicht unberücksichtigt bleiben dürfen. Grundvoraussetzung für die Verfügbarkeit sind schnelle und stabile Internet-Zugänge und -Verbindungen. Kurzfristige Ausfälle bei Cloud-Anbietern haben Kunden in der Vergangenheit in arge Probleme gestürzt. Zudem macht die Datensicherheit vielen Unternehmen Sorgen: Sie wollen nicht riskieren, dass Daten verlorengehen oder vertrauliche Informationen in fremde Hände geraten. Schließlich muss es möglich sein, die Daten problemlos von einem Anbieter zu einem anderen zu übertragen. Deshalb ist es unerlässlich, bei der Auswahl eines Cloud Computing Anbieters besonders sorgfältig zu sein und sich genau darüber zu informieren, welche Sicherheitsstandards gelten und welche Datenschutzmaßnahmen ergriffen werden.

2.4.2. Vor- & Nachteile des Einsatzes von Cloud Computing?

Cloud Computing ist weder ausschließlich mit Nachteilen behaftet noch ein Allheilmittel. Es ist immer genau zu prüfen, ob ein Cloud-Dienst im Einzelfall die richtige Wahl ist.

Eine Cloud-Lösung kann viele Vorteile bieten. So sind Ressourcen leicht & dynamisch an den anfallenden Bedarf anpassbar. Für den Einsatz einer Cloud sprechen meist:

\ Kostenreduktion
\ Flexibilitätssteigerung
\ Wenn das Angebot keine technischen

Anpassungen erfordert, ermöglicht es eine Entlastung der eigenen IT-Infrastruktur sowohl in personeller als auch in sachlicher Hinsicht.

Doch es gibt auch Nachteile. So flexibel die Preisstruktur so unflexibel ist meist das angebotene Produkt:

\ Leistungen sind standardisiert, eine Konfiguration nur im Rahmen vorgesehener Optionen möglich;
\ Verträge sind in wesentlichen Teilen nicht verhandelbar;
\ Lock-in-Effekt[5] und reduzierte Kontrolle

2.4.3. Was nimmt der Cloud-Dienst nicht ab?

Die datenschutzrechtliche Verantwortung bleibt beim Auftraggeber. Die Fragen, die daher unbedingt gestellt werden müssen, sind:

\ Was sind meine Leistungsanforderungen?
\ Kann ich meinen Kontrollpflichten entsprechend dem DSG bzw. der DS-GVO gerecht werden?
\ Ist der Cloud-Dienst mit meiner IT-Landschaft kompatibel?
\ Sind technische und vertragliche Vorgaben überprüfbar?

[4] Eine Erläuterung der verschiedenen Cloud-Arten finden Sie im Angang.

[5] Bindung an Produkte/Dienstleistungen/Anbieter, die einen Wechsel wegen entstehender Wechselkosten oder sonstiger Wechselbarrieren erschweren.

3. Beschäftigtendatenschutz

Das digitale Zeitalter ist geprägt von ständiger Veränderung, an die sich der WDR in Bezug auf Arbeitsabläufe, Programmgestaltung und Verbreitung kontinuierlich anpassen muss.

3.1. Einführung der digitalen Personalakte

Die Personalabteilung hat insbesondere mit dem Themenbereich Digitale Personalakte damit begonnen, ihre Abläufe auf digitale Prozesse umzustellen. Das archivierte Personalaktenmaterial soll auf eine digital geführte Ablage im betriebswirtschaftlichen System SAP HR umgestellt werden. Hierdurch ist ein standortunabhängiger digitaler Zugriff auf die Personalakten möglich.

Zunächst müssen für dieses Projekt die bislang im Papier vorgehaltenen Akten digitalisiert werden. Dieser Prozess der Aktenaufbereitung soll von einer Fremdfirma übernommen werden. Um eine Datenschutzkonformität der Digitalisierung durch die avisierte Fremdfirma zu gewährleisten, hat Günter Grießbach als Vertreter des Datenschutzreferats bei einer Besichtigung zusammen mit den zuständigen Kollegen von Personalabteilung, Anwendungsmanagement sowie Personalrat bei dem Dienstleister eine datenschutzrechtliche Prüfung der technischen und organisatorischen Maßnahmen der Datensicherung nach § 10 DSG NRW durchgeführt.

Die Kollegen konnten vor Ort anhand von Beispielen besichtigen, wie eine Personalakte die einzelnen Prozessschritte von Transport über Lagerung, Aufbereitung, Scannen der Akten, Klassifizierung und Erfassung des Datums des Scans, Qualitätssicherung des Digitalisierungsergebnisses, Archivierung bis hin zu Speicherung der digitalen Ergebnisdateien und Vernichtung der Originalunterlagen durchläuft und dies datenschutzrechtlich bewerten. Dabei stellten sie fest, dass bei der Pflege und Aktenaufbereitung ein sehr hoher manueller Aufwand erforderlich werden würde, den man zurzeit technisch nicht bewältigen kann. Aus diesem Grund wurden zusätzliche organisatorische Sicherheitsvorkehrungen besprochen. So ist das bei sich Führen von Mobilgeräten und Kameras oder dergleichen der Mitarbeiter während der Prozessschritte nicht zugelassen und es gibt auch keine PCs / Laptops in diesen Aufbereitungsräumen, um zu verhindern, dass Daten unerlaubt nach außen gegeben werden können. Weitere die Datensicherheit betreffende Fragen, wie zum Beispiel wie viele Mitarbeiter sind mit der Digitalisierung befasst, wie sieht das Notfallkonzept bei Störungen aus, was passiert bei einem Datenverlust, wie sehen Verfahrensverzeichnis und Berechtigungskonzept aus, wurden vom Dienstleister zufriedenstellend beantwortet. Damit bestanden aus Sicht des Datenschutzreferates keine Einwände, die Personalakten wie geplant digitalisieren zu lassen.

Im zweiten Schritt mussten die internen datenschutzrechtlichen Vorgaben mit allen Projektbeteiligten erörtert werden. Zur Sicherstellung eines datenschutzkonformen Prozesses wurde insoweit von Personalabteilung und Personalrat in enger Abstimmung mit dem Datenschutzreferat eine Dienstvereinbarung erarbeitet, in der neben Ziel und Zweck der Digitalen Personalakte und Einsichtsrechten von Mitarbeitern unter anderem eine Berechtigungsmatrix zwischen den Parteien abgestimmt wurde, die regelt, wer beim Go Live wie auf welche Inhalte der Personalakte welchen Zugriff erhalten wird.

3.2. Betriebliches Gesundheitsmanagement (BGM)

Ein weiteres datenschutzrechtlich relevantes Thema des Beschäftigtendatenschutzes ist das BGM. Da es sich bei Gesundheitsdaten, um besondere personenbezogene Daten im Sinne von § 4 Absatz 3 DSG NRW handelt, ist eine Einbeziehung des Datenschutzes in diesem Bereich besonders wichtig. Nach § 4 Absatz 3 Ziffer 4 a) in Verbindung mit § 29 Absatz 1 Satz 1 DSG NRW ist eine Weitergabe von Daten im Dienst- oder Arbeitsverhältnis nur zulässig, wenn dies zur Durchführung organisatorischer, personeller oder sozialer Maßnahmen erforderlich ist.

Grundsätzlich muss insoweit das vom Arbeitgeber freiwillig durchgeführte BGM strikt von dem gesetzlich vorgeschriebenen Betrieblichen Eingliederungsmanagement (BEM) unterschieden werden. Das BGM bedient sich statistischer Werte, um strukturelle Veränderungen zur Verbesserung der Gesundheit bei Mitarbeitergruppen vornehmen zu können. Dafür ist eine personenbezogene Auswertung gerade nicht nötig. Ohne Personenbezug befinden wir uns außerhalb des Anwendungsbereichs des Datenschutzrechts. Das nur in groben Zügen gesetzlich normierte Betriebliche Eingliede-

rungsmanagement (BEM) erhebt dagegen personenbezogen auf den Einzelfall Krankheitsdaten, die über das dem Arbeitgeber normalerweise bekannte Maß deutlich hinausgehen können.

Grundsätzlich muss ein Beschäftigter seinem Arbeitgeber keine Auskunft über die Art seiner Erkrankung geben. Anders kann es im Rahmen eines BEM sein, wenn es Anhaltspunkte dafür gibt, dass die Arbeit bei der Erkrankung eine Rolle spielt. Damit der Arbeitgeber in solchen Fällen durch ein frühzeitiges Zugehen auf erkrankte Arbeitnehmer die Möglichkeit hat, schnellstmöglich eventuellen gesundheitlichen Gefährdungen am Arbeitsplatz entgegenzuwirken, sieht § 84 Absatz 2 SGB IX das sogenannte BEM vor. Es wird jedem Beschäftigten angeboten, der innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig war. Der Arbeitgeber muss das Gespräch anbieten, der Beschäftigte ist aber nicht verpflichtet, die Einladung zum BEM-Gespräch anzunehmen. Eine personenbezogene Datenerhebung für BEM-Gespräche im Sinne von § 84 Absatz 2 SGB IX ist damit anlassbezogen und freiwillig.

Aufgabe des Datenschutzes ist es im Zusammenhang mit einem BEM die widerstreitenden Interessen der Beteiligten miteinander in Einklang zu bringen. Es muss sichergestellt sein, dass die für den Arbeitgeber erforderlichen Daten datensparsam erhoben werden. So darf gemäß § 28 Absatz 1 BDSG, § 29 Absatz 1 DSG NRW beispielsweise in der Personalakte alles vermerkt werden, was zum Nachweis der Durchführung eines ordnungsgemäßen BEM erforderlich ist, das ja eine Arbeitgeberpflicht darstellt. Erforderlich ist insofern die Dokumentation des Angebots zur Durchführung eines BEM, aber auch das Einverständnis/Nichteinverständnis der betroffenen Person. Sofern die Darstellung der im Rahmen des BEM gefundenen Maßnahmen keine Rückschlüsse auf die konkrete Erkrankung zulässt, dürfen sogar angebotene und vorgenommene konkrete Maßnahmen in der Personalakte hinterlegt werden.

Auf der anderen Seite muss der Arbeitnehmer sicher darauf vertrauen dürfen, dass die im Zusammenhang mit einem BEM erhobenen, unter Umständen extrem sensiblen Daten, vertrauensvoll behandelt werden. Bereits im Schreiben, mit dem ein BEM-Gespräch angeboten wird, muss transparent gemacht werden, welche Daten im Verlauf des BEM unter welchen Voraussetzungen erhoben und wem sie bekannt gemacht werden.

Im Zusammenhang sowohl mit dem BGM als auch den Prozessen zum BEM gibt es aufgrund der unterschiedlichsten Fallkonstellationen immer wieder Klärungsbedarf datenschutzrechtlicher Fragestellungen. Wir sind hier im engen Austausch mit Personalabteilung und betrieblichem Gesundheitsmanagement.

3.3. Telearbeit Beihilfe/ Rheinische Versorgungskasse (RVK)

Ende 2014 ergab eine Prüfung der RVK keinen Anlass für Beanstandungen, wie dem 23.Tätigkeitsbericht (dort Ziff. 2.3) zu entnehmen ist. Anlässlich einer neuerlichen Prüfung durch die Kollegen vom Zentralen Beitragsservice wurden wir jedoch darauf aufmerksam gemacht, dass Beihilfebearbeitungen durch die RVK in Telearbeit erfolgen, was seitens des Datenschutzreferats des Zentralen Beitragsservice als datenschutzrechtlich sehr kritisch bewertet wurde.

Da sich der Zentrale Beitragsservice in Köln befindet, wurde ich von der Datenschutzbeauftragten des Zentralen Beitragsservice, als für den Schutz der Daten der Mitarbeiter des Zentralen Beitragsservice zuständige Datenschutzaufsicht der Sitzanstalt, eingeschaltet. Da sich meine Aufsichtsfunktion allein auf den WDR und in diesem Fall auf den Zentralen Beitragsservice bezieht, habe ich nach erfolglosen Gesprächen mit der RVK die Landesbeauftragte NRW, die als Datenschutzaufsichtsbehörde der RVK fungiert, eingeschaltet.

Nach Auffassung der Landesdatenschutzbeauftragten, die im 14. Datenschutzbericht LDI NRW von 1999[6] auf Seite 132 niedergelegt wurde, „sollten personenbezogene Daten, die Berufs- oder besonderen Amtsgeheimnissen unterliegen, nicht in Tele-Heimarbeit verarbeitet werden. Hierzu zählen insbesondere Sozial-, Personal- und Steuerdaten sowie Beihilfedaten und medizinische Daten.“ Diese Auffassung wurde mir telefonische vom Leiter des Referats 3 für Beschäftigtendatenschutz im öffentlichen Bereich, Gesundheit und den Sozialbereich als aktuell bestätigt.

Ich habe deshalb von meinem Anrufungsrecht gemäß § 25 DSG NRW Gebrauch gemacht. Die Landesaufsicht prüft derzeit den Sachverhalt. Über den weiteren Fortgang in dieser Sache sowie die Stellungnahme der Landesdatenschutzbeauftragten werde ich im nächsten Tätigkeitsbericht berichten.

[6] https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/14_DSB/14__Datenschutzbericht.pdf

4. Datenschutz im journalistisch-redaktionellen Bereich

4.1. Social-Media-Leitfaden

Der AK DSB hat im September 2016 einen Leitfaden Social Media in die Häuser gebracht. Dieser richtet sich an Mitarbeiter, die Telemedien- und Social-Media-Angebote redaktionell einsetzen und technisch realisieren. Er konkretisiert datenschutzrechtliche Vorgaben und soll Orientierung bieten. Er soll Telemedienverantwortlichen dabei helfen, datenschutzrelevante Themen zu erkennen, zu beurteilen und mit datenschutzrechtlichen Vorgaben verantwortungsvoll umzugehen.

Den Leitfaden finden Sie bei Interesse im Anhang (Ziffer 7.2) dieses Berichts. Er wird derzeit im Hinblick auf die Vorgaben der DS-GVO aktualisiert.

4.2. Cookies und ePrivacy

Ein Aktualisierungsbedarf wird sich aller Voraussicht nach insbesondere in Bezug auf Cookies im Zusammenhang mit der Nutzungsmessung ergeben. Zum 25. Mai 2018, also parallel zum Wirksamwerden der DS-GVO, soll eine neue ePrivacy Verordnung in Kraft treten. Die E-Privacy-Verordnung wird alle Regelungen, die auf Grundlage der E-Privacy-Richtlinie[7] ergangen sind, wie beispielswiese die sogenannte Cookie-Richtlinie[8], verdrängen und die rechtlichen Rahmenbedingungen der Messung des Nutzerverhaltens neu regeln. Die ePrivacy Verordnung wurde Anfang 2017 von der EU-Kommission als offizieller Entwurf vorgestellt.[9] Sie wird wie die DS-GVO als Verordnung keiner weiteren Umsetzung in nationales Recht der Mitgliedsstaaten bedürfen.

Bisher gilt in Deutschland gemäß § 15 Absatz 3 TMG für die Verwendung von Cookies die sogenannte Opt-Out-Lösung. Danach ist es ausreichend, dass Unternehmen, welche Nutzungsprofile auf pseudonymer Basis erstellen, beim Aufruf der Webseite hierüber in der Datenschutzerklärung informieren und den Nutzern die Möglichkeit geben, der Erstellung von Nutzungsprofilen zu widersprechen. Diese Regelung wird ersatzlos gestrichen.

Möchte man weiter Cookies setzen, so würde sich dies künftig nach den Vorgaben des neuen Artikel 8 Absatz 1 des offiziellen Entwurfs zu richten haben. Laut Buchstabe a) wäre das Setzen von Cookies möglich, soweit es für die Durchführung des elektronischen Kommunikationsvorgangs nötig ist, nach Buchstabe b), sofern der Endnutzer seine Einwilligung gegeben hat, c) es für die Bereitstellung des vom Endnutzer gewünschten Dienstes oder d) es für die Messung des Webpublikums nötig ist.

Hinsichtlich des Setzens von Cookies zu Marktforschungszwecken oder für eine Personalisierung von Angeboten besteht derzeit eine gewisse Unsicherheit, wie sich die Haltung der Verordnungsgeber hierzu verhält. Was die Verordnung also letztendlich im Einzelnen für den WDR bedeuten wird, bleibt zum jetzigen Zeitpunkt abzuwarten.

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

[8] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

[9] https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

5. Rundfunkteilnehmer-datenschutz

5.1. Meldedatenabgleich, Rundfunkbeitragsstaatsvertrag und DS-GVO

Beim Zentralen Beitragsservice laufen die Vorbereitungen für den für Mitte nächsten Jahres geplanten erneuten Meldedatenabgleich. Im kommenden Herbst findet ein Treffen mit den Rundfunkdatenschutzbeauftragten und den zuständigen staatlichen Datenschutzbeauftragten statt, bei dem die konkreten Pläne erläutert werden.

Bislang gibt es keinen neuen Stand bei den Überlegungen zur Notwendigkeit der Anpassung des Rundfunkbeitragsstaatsvertrages an die DS-GVO. Besondere Bedeutung kommt den sich aus der DS-GVO ergebenden Benachrichtigungspflichten im Zusammenhang mit der Durchführung des zweiten Meldedatenabgleichs zu. Mit diesem Thema ist die Unterarbeitsgruppe „Datenschutz bei der Rundfunkteilnehmerdatenverarbeitung“ befasst.

5.2. Anfragen und Auskunftsersuchen

Jeder kann sich an das Datenschutzreferat des WDR wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch den WDR in seinen schutzwürdigen Belangen verletzt worden zu sein. Die das Datenschutzreferat von außen erreichenden Themen und Anfragen sind vielfältig, vermehrt jedoch leider auch Themen, bei denen ich nicht helfen kann.

Die allermeisten Anfragen erreichen uns im Beitragszusammenhang. Oft handelt es sich um Befreiungs- oder Abmeldebegehren, die wir zuständigkeitshalber an die entsprechenden Service-Nummern des Beitragsservice weiterleiten müssen. Soweit allgemein die Zulässigkeit einer Datenerhebung durch den Zentralen Beitragsservice bezweifelt wird, werden diese Anfragen vom Datenschutzreferat des Zentralen Beitragsservice von ARD, ZDF und Deutschlandradio in meinem Auftrag beantwortet. Eingaben aus dem WDR-Sendegebiet, die über einen solchen Routineschriftwechsel hinausgehen, beantworte ich selbst.

Auch Begehren das Programm betreffend haben mich im letzten Jahr vermehrt erreicht. Diese darf ich aufgrund des Medienprivilegs soweit es um die Zulässigkeit der Datenerhebung geht, datenschutzrechtlich nicht bewerten. Nach § 49 WDR-Gesetz, wie eingangs bereits ausführlich geschildert, finden Bestimmungen über den Datenschutz auf personenbezogene Daten, die ausschließlich eigenen journalistisch-publizistischen Zwecken des WDR dienen, nur betreffend der Datensicherungsvorschriften Anwendung. Ich bin im journalistischen Bereich demnach nur aufsichtsberechtigt, soweit eine Verletzung von Datensicherungsvorschriften geltend gemacht wird. Das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt greift jedoch gerade nicht, weshalb Anfragende, die ihre Person betreffende Veröffentlichung zu verhindern suchen, an die zuständige Redaktion oder die Publikumsstelle beim Intendanten verwiesen werden müssen.

Auch wenn die Wahl von Kommunikationsmitteln und Übertragungswegen durch den WDR kritisiert wird (beispielsweise Kritik an der Präsenz des WDR auf Facebook oder an der Durchführung von Umfragen via Whats App), sind wir nicht zum Einschreiten befugt. Dies liegt im alleinigen Ermessen der redaktionellen Kollegen des WDR. Wir stellen insofern sicher, dass die Kommunikationsmittel datensicher und wie in den Datenschutzerklärungen beschrieben, umgesetzt werden.

6. Zusammenarbeit und Informationsaustausch

6.1. AK DSB

Zur Koordinierung der datenschutzrechtlichen Kontroll- und Beratungstätigkeit im Bereich des öffentlich-rechtlichen Rundfunks treffen sich die Datenschutzbeauftragten von ARD, ZDF, Deutsche Welle, Deutschlandradio und die betriebliche Datenschutzbeauftragte des zentralen Beitragsservice zweimal jährlich. Zusätzlich werden besonders aktuelle und dringende Themen in Telefonkonferenzen beraten. Dieses Rundfunk-Datenschutz-Forum, das seit 1979 besteht, bietet Gelegenheit, Erfahrungen auszutauschen und anstaltsübergreifende Projekte gemeinschaftlich datenschutzkonform abzuwickeln. Hier werden auch die Interessen und Meinungen im Sinne der Mitwirkung bei gesetzgeberischen Vorhaben im Medien- und Datenschutzbereich gebündelt. Um einzelnen Themen in besonderem Maße gerecht zu werden, wirken verschiedene Mitglieder des AK DSB zusätzlich in themenbezogenen Unterarbeitskreisen mit. Darüber hinaus ist auch der Datenschutzbeauftragte des Österreichischen Rundfunks (ORF) mit dem AK DSB verbunden und nimmt regelmäßig an den Sitzungen teil.

Im zweijährigen Turnus wechselt der Vorsitz im Arbeitskreis. Im Berichtszeitraum hatte zunächst der Datenschutzbeauftragte des ZDF, Herr Christoph Bach, den Vorsitz. Nachdem er sein Amt Mitte 2016 aufgrund der Übernahme einer anderen Funktion aufgab, hat Herr Horst Brendel, Datenschutzbeauftragter des NDR, den Vorsitz im AK DSB übernommen. Im November 2016 ist der Vorsitz auf den Datenschutzbeauftragten des MDR, Herrn Stephan Schwarze, übergegangen.

Da an den verschiedensten Stellen dieses Berichts bereits über wichtige Beratungsthemen des AK DSB berichtet wurde, möchte ich an dieser Stelle nur noch kurz auf das Thema „Bring your own device“ (BYOD) eingehen.

BYOD meint die Nutzung privater, zumeist mobiler Endgeräte für dienstliche Zwecke. Ob und für welche Zwecke BYOD im Unternehmen erlaubt wird, ist eine Management-Frage, die zumindest im WDR lange Zeit mit nein beantwortet wurde. Sowohl die Sparzwänge des öffentlich-rechtlichen Rundfunks als auch wachsende Begehrlichkeiten insbesondere freier Mitarbeiter, bringen dieses Thema aber in den verschiedensten Facetten immer wieder aufs Tableau. Aus diesem Grund hat der AK DSB eine Projektgruppe BYOD für die Beantwortung der datenschutz-rechtlichen Grundfragen gegründet.

6.2. Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder

Aus der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist unter anderem der Arbeitskreis Medien (AK Medien) hervorgegangen, der sich mit Themen speziell aus den Bereichen Datenschutz und Medien beschäftigt.

Der AK Medien arbeitet mit dem AK DSB in einer kleinen gemeinsamen Arbeitsgruppe zusammen. Hier kommen ausgesuchte, beide Seiten tangierenden Themen zwischen den Vertretern beider Kreise in kleiner Gruppe zur Diskussion. Ein erstes Treffen der Arbeitsgruppe hat Anfang 2017 zum Thema Jugendmedienschutz stattgefunden.

6.3. Arbeitskreis IT-Sicherheit

Der Datenschutzbeauftragte des SWR berichtet als ehemaliger IT-Sicherheitsbeauftragter regelmäßig über die Sitzungen des Arbeitskreises. Ich selbst bin regelmäßiges Mitglied der WDR-internen Sitzungen der IT-(Bereichs)Sicherheitsbeauftragten, in die die Themen des Arbeitskreises ebenfalls kommuniziert werden.

Die Zusammenarbeit zwischen Datenschutz- und IT-Sicherheit wird sich perspektivisch durch die Vorgaben der DS-GVO weiter erhöhen.

6.4. IVZ und ARD/ZDF-Box

Das Informationsverarbeitungszentrum (IVZ) ist eine Gemeinschaftseinrichtung von BR, DW, DRadio, hr, MDR, NDR, RB, rbb, SR, SWR und WDR. Als Datenschutzbeauftragte eines Kooperationspartners dieser

Gemeinschaftseinrichtung obliegt mir die diesbezügliche datenschutzrechtliche Aufsichtszuständigkeit, soweit Daten des WDR verarbeitet werden.

Das IVZ betreibt unter anderem die sogenannte ARD / ZDF-Box, die den Kooperationspartnern eine datenschutzkonforme Alternative zu Filehosting-Diensten, wie DropBox, Google Drive, MS OneDrive oder iCloud bietet.

Der Wunsch Daten einfach, komfortabel und schnell zu übermitteln und Berechtigungen an Dokumenten, Fotos und Audio-Dateien individuell vergeben zu können, war groß. Die auf dem Markt erhältlichen Tools aber als Public-Cloud-Anwendung mit potentiell weltweitem Speicherort nicht datenschutzkonform nutzbar. Zu den diesbezüglichen Problemen mit amerikanischen Produkten, sei auf die Ausführungen unter 2.1 verwiesen.

Die ARD-Box speichert die Daten auf den Servern des IVZ und setzt sie damit nicht dem Zugriff von unbefugten Dritten aus. Bei der Entwicklung dieser datenschutzkonformen Lösung hat der AK DSB eng mit dem IVZ zusammengearbeitet und beraten, so dass es nun ein sicheres und datenschutzgerechtes Angebot gibt, das den Anforderungen aller Beteiligten entspricht und eine gute und sichere Alternative zu den auf dem Markt erhältlichen Filehosting Diensten bietet.

7. Anhang

7.1. Cloud-Arten

Infrastructure as a Service (IaaS)

Diese unterste Ebene, auch Cloud Foundation genannt, umfasst alle IT-Leistungen der Basisinfrastruktur. Dazu zählen unter anderem Rechnerkapazitäten, Netzwerke und Speicherplatz. Der große Vorteil von IaaS im Gegensatz zu herkömmlichen Angeboten liegt in der Skalierbarkeit: Die Cloud Dienste können je nach Nutzungsgrad und Bedarf dynamisch angepasst werden. So kann zum Beispiel in Anspruch genommener Speicherplatz jederzeit erweitert oder verkleinert werden.

Platform as a Service (PaaS)

Eine Ebene über der Infrastructure as a Service liegen IT-Leistungen, mit denen sich Anwendungssoftware und -komponenten entwickeln und integrieren lassen. Der Cloud Service bietet in diesem Fall eine Programmierschnittstelle beziehungsweise einen Zugang zu einer Software-umgebung, in der Entwickler Anwendungssoftware erstellen und über Cloud Dienste anbieten.

Software as a Service (SaaS)

Die oberste Ebene, auch oft als Software on demand bezeichnet, umfasst Anwendungen, die über Cloud Dienste bereitgestellt werden. Da-bei bieten Cloud Computing Anbieter spezielle Anwendungssoftware an, die auf ihrer IT-Infrastruktur läuft.

Private Cloud

Bereitstellung von Cloud Diensten aus einem unternehmenseigenen Rechenzentrum.

Hauptmerkmal einer „Private Cloud“ ist, dass sich Anbieter und Nutzer der Cloud kennen und meist auch im selben Unternehmen befinden. Die Private Cloud wird im Unternehmen selbst kontrolliert und betrieben, und die Dienste sind nur für eine beschränkte Anzahl an Personen, beispielsweise Mitarbeiter und autorisierte Geschäftspartner, zugänglich. Der Zugriff auf Dienste und Anwendungen in einer Private Cloud erfolgt meist über das Intranet oder, wenn sich die Nutzer außerhalb des Unternehmens befinden, über eine VPN-Verbindung (Virtual Private Network). Es gelten Dienstvereinbarungen und gesetzliche Datenschutzrichtlinien.

Zum Beispiel in der ARDBox, ARD Cloud (gemeinschaftliche Entwicklung mit dem IRT und ARD,ZDF)

Public Cloud

Bereitstellung von Cloud Diensten aus einem öffentlich zugänglichen System.

Eine Public Cloud wird von einem externen IT-Dienstleister betrieben. Sie ist öffentlich, kann also von vielen Personen und Unternehmen über das Internet genutzt werden. Es wird hierbei zwischen zwei unterschiedlichen Formen der Public Cloud unterschieden: Apple Cloud, MS Cloud, Trello (Planungsplattform für Projekte)

Cloud Computing wird in nächster Zeit mit Sicherheit noch weiter an Bedeutung zunehmen und dabei eine Vielzahl von Arbeits- und Geschäftsprozessen erleichtern und optimieren.

Open Cloud

Hier kennen sich Anbieter und Nutzer nicht und haben auch keinen direkten Kontakt zueinander und keine vereinbarten Richtlinien zum Schutz der Daten. Dies birgt ein potenzielles Risiko in Bezug auf das Thema Datenschutz. Der Nutzer hat meist keine Kenntnis über den Standort oder dem Server, auf denen seine Daten verarbeitet werden. Gerade bei Opensource Software wie beispielsweise DropBox, Slack, Trello, Google Drive ist dies nicht unerheblich.

Exclusive Cloud

Anbieter und Nutzer einer Exclusive Cloud hingegen kennen sich. Sie handeln feste Bedingungen und Konditionen aus und schließen einen verbindlichen Vertrag darüber ab.

Die Vorteile liegen auf der Hand: Jede Person beziehungsweise jedes Unternehmen wurde vor der Nutzung eindeutig identifiziert und vom Anbieter autorisiert. In den Nutzungsbedingungen und Datenschutzbestimmungen, denen jeder Nutzer zustimmen muss, wird unter anderem auch der Standort aller an dem Cloud-Service beteiligten Server angegeben. Zum Beispiel in der ARDBox, ARD Cloud (gemeinschaftliche Entwicklung mit dem IRT und ARD,ZDF)

In diesem Zusammenhang und aufgrund Flexibilität und Kostenersparnis, wird Cloud Computing in nächster Zeit mit Sicherheit noch weiter an Bedeutung zunehmen.

7.2. Social-Media-Leitfaden

LEITLINIEN ZUM DATENSCHUTZ IN DEN TELEMEDIEN- UND SOCIAL-MEDIA-ANGEBOTEN DER RUNDFUNKANSTALTEN

Vorbemerkung

Was will Datenschutz?

Datenschutz ist ein Grundrecht, das die Privatsphäre schützt.

Freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Verarbeitung und Weitergabe seiner personenbezogenen Daten voraus. Datenschutz ist das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (sogenanntes Recht auf informationelle Selbstbestimmung). Geschützt wird damit die Freiheit des Einzelnen, selbst zu entscheiden, wer was wann und bei welcher Gelegenheit über ihn weiß. Das Internet und die zunehmende Digitalisierung stellen den Datenschutz dabei vor neue Herausforderungen. Das Wachstum des Internets geht mit einem stetigen Anstieg der gesammelten personenbezogenen Daten einher.

Was will der Leitfaden?

Dieser Leitfaden ist ein Ratgeber und richtet sich an die Mitarbeiter[10], die Telemedien- und Social Media-Angebote redaktionell einsetzen und technisch realisieren. Er konkretisiert die verbindlichen Vorgaben der Datenschutzgesetze und der einschlägigen Rechtsprechung für öffentlich-rechtliche Telemedien- und Social Media-Angebote.

Der Leitfaden soll eine Orientierung bieten und den Telemedienverantwortlichen in den Rundfunkanstalten dabei helfen, datenschutzrelevante Themen zu erkennen, zu beurteilen und sie mit datenschutzrechtlichen Vorgaben verantwortungsvoll in Einklang zu bringen. Der Leitfaden ersetzt jedoch nicht die Beratung mit dem zuständigen Datenschutzbeauftragten, der im Zweifel hinzuzuziehen ist.

Der Leitfaden bietet mit den „Datenschutz Basics“ einen Überblick über die wichtigsten datenschutzrechtlichen Grundprinzipien. Daneben liegt der Fokus auf praxisrelevanten Einzelthemen von A wie Apps bis W wie Webanalyse. Anhand von Checklisten wird dabei für jedes Thema dargestellt, worauf für eine datenschutzkonforme Realisierung zu achten ist. Oftmals sind hier neben dem Datenschutz noch andere rechtliche Aspekte zu beachten; diese sind in Rücksprache mit den zuständigen Justitiariaten zu klären.

Datenschutz „Basics“

Welche Grundgedanken stehen hinter den Anforderungen, die der Datenschutz an die Rundfunkanstalten für ihre Telemedienangebote stellt? Mit ein paar Grundprinzipien kann man sich auch im komplizierten Datenschutzrecht gut zurechtfinden.

Sind die Daten personenbezogen?

Die Regelungen des Datenschutzrechts kommen nur dann zur Anwendung, wenn die Rundfunkanstalt „personenbezogene Daten“ von Nutzern speichert und nutzt.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Darunter versteht man alle Daten, die dazu genutzt werden können, die Identität des Users offen zu legen. Dazu gehört nicht nur der richtige Name, Anschrift, Telefonnummer oder eine E-Mail-Adresse. Auch andere Informationen wie zum Beispiel die IP-Adresse, Standortdaten, Gerätekennungsnummern sowie sonstige Informationen (zum Beispiel über das Nutzungsverhalten) sind ebenfalls relevant, weil sie zumindest personen*beziehbar* sind.[11]

Wer ist die für die Datenverarbeitung „verantwortliche Stelle“?

Wenn die Rundfunkanstalt in ihren Telemedienangeboten personenbezogene Daten von Nutzern verarbeitet,

[10] Zur besseren Lesbarkeit wird im Folgenden ausschließlich eine Bezeichnungsform verwendet. Selbstverständlich sind alle Formulierungen für alle Geschlechter gleichermaßen zutreffend.

[11] Aufgrund der aktuellen Rechtsprechung und im Einklang mit der Auffassung der deutschen Aufsichtsbehörden im Datenschutz sind statische **und** dynamische IP-Adressen als personenbezogene Daten zu werten.

ist sie gemäß den Datenschutzgesetzen die „verantwortliche Stelle“ und damit verantwortlich für die datenschutzkonforme Gestaltung ihrer Angebote.

Dies gilt auch, wenn sich die Rundfunkanstalt bei der Umsetzung einer Webseite, dem Hosting oder der App-Programmierung eines externen Dienstleisters bedient, der im Auftrag der Anstalt tätig wird (siehe hierzu die Hinweise zur Auftragsvergabe an Dritte).

Sofern die Rundfunkanstalt in ihren Angeboten Tools und sonstige Inhalte von externen Dritten einbindet, bleibt sie jedenfalls insofern rechtlich verantwortlich, dass sie dafür sorgen muss, dass die Übertragung von Daten der Nutzer an Dritte mit dem Wissen und Wollen der Nutzer erfolgt (siehe hierzu die Hinweise zum Embedding von fremden Inhalten).

Ist die Rundfunkanstalt auf einer Drittplattform präsent, ist grundsätzlich der jeweilige Plattformanbieter für die Datenverarbeitung datenschutzrechtlich verantwortlich (siehe hierzu die Hinweise zu Drittplattformen).[12]

Rechtmäßigkeit der Datenerhebung und -nutzung

Werden personenbezogene Daten gespeichert und verarbeitet, bedarf dies stets einer Erlaubnis. Eine solche Erlaubnis kann sich entweder aus einer Rechtsvorschrift, einem Vertrag oder aus einer ausdrücklichen Einwilligung des Nutzers ergeben.

Die datenschutzrechtliche Zulässigkeit der Datenverarbeitung lässt sich nicht pauschal beurteilen, sondern muss anhand des jeweiligen Einzelfalls geprüft werden.

Der Leitfaden gibt für verschiedene typische Fragestellungen eine Orientierung, was die Rundfunkanstalten zu beachten haben.

Einwilligung des Nutzers

Sofern die Erhebung von personenbezogenen Daten nicht per Gesetz erlaubt ist, ist grundsätzlich eine Einwilligung des Nutzers notwendig. Für eine wirksame Einwilligung ist auf folgendes zu achten:

\ Der Nutzer ist *vor* Beginn der Datenverarbeitung umfassend zu informieren.

\ Der Text der Einwilligungserklärung muss dem Nutzer klar und allgemein verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die Rundfunkanstalt informieren.

\ Der Einwilligungstext muss klar und eindeutig formuliert sein, so dass der Nutzer erkennen kann, was er hier erklärt („*Ich willige ein, dass ...*“; „*Ich bin einverstanden, dass ...*“).

\ Es muss sich um eine bewusste Erklärung handeln (Opt-in). Diese kann zum Beispiel im Wege eines Häkchens in einer Checkbox abgegeben werden. Aber: Im Sinne einer Zustimmung *vorangekreuzte* Einwilligungstexte oder nur mit einer Streich-/Abwahl-Möglichkeit versehene „vorgegebene“ Zustimmungen (Opt-out) genügen nicht.

\ Sollen besonders sensible persönliche Daten erhoben und verarbeitet werden, ist der Nutzer darüber im Zuge seiner Einwilligung gesondert zu unterrichten. Dies ist zum Beispiel der Fall bei: Angaben über die ethnische Herkunft; politische Meinungen; religiöse und philosophische Überzeugungen, Daten zu Gesundheit und Sexualleben; Daten über Straftaten.

\ Eine wirksame Einwilligung liegt nur vor, wenn diese freiwillig abgegeben wird. Eine unter Druck oder Zwang abgegebene Einwilligung ist unwirksam.

\ Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt, muss die Einwilligung protokolliert werden und jederzeit für den Nutzer abrufbar sein. Es ist ausreichend, wenn die Einwilligung jeweils auf Anfrage zugänglich gemacht wird.

\ Die Einwilligung muss jederzeit in einfacher Weise vom Nutzer widerrufbar sein. Der Nutzer ist über sein Widerrufsrecht zu informieren. Die Unterrichtung kann zum Beispiel in der allgemeinen Datenschutzerklärung erfolgen.

\ Die datenschutzrechtliche Einwilligung zu einer konkreten Datenverarbeitung ist deutlich zu trennen von den generellen Datenschutzhinweisen in einem Telemedienangebot mit reinen Informationen über Datenverarbeitung auf gesetzlicher Grundlage (siehe hierzu die Hinweise zur Datenschutzerklärung). Besonderheiten gelten bei der Datenverarbeitung von Minderjährigen (Hinweise zum Minderjährigen-Datenschutz).

[12] Aufgrund der aktuellen Rechtsprechung ist davon auszugehen, dass auch der Betreiber einer Facebook-Fanpage keine verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist.

Grundsatz der Zweckbindung und Erforderlichkeit

Jeder Umgang mit personenbezogenen Daten muss einen ganz bestimmten Zweck verfolgen. Die Daten dürfen nur gespeichert und verarbeitet werden, soweit diese Verarbeitung für den jeweiligen Zweck erforderlich ist. Eine pauschale Abfrage und Nutzung von persönlichen Daten eines Nutzers ohne Verfolgung eines konkret festgelegten Zwecks ist daher nicht zulässig. Eine Verwendung der Daten für andere Zwecke ohne Wissen und Einverständnis des Nutzers ist ebenfalls nicht zulässig.

Sobald die personenbezogenen Daten nicht mehr zu dem ursprünglich angegebenen Zweck benötigt werden, müssen sie grundsätzlich gelöscht werden. Das gleiche gilt im Falle des Widerrufs einer Einwilligungserklärung in die Datenverarbeitung durch den Nutzer.

Aber: Unabhängig vom Datenschutz können gesetzliche Aufbewahrungspflichten bestehen (zum Beispiel nach den Vorgaben der Abgabenordnung oder des Handelsgesetzbuches). In diesem Fall sind die Daten zu sperren und damit von den aktuellen Produktivdaten zu trennen.

Grundsatz der Datenvermeidung und Datensparsamkeit

Es sollen immer so wenig personenbezogene Daten wie möglich für den konkreten Zweck abgefragt werden. Dabei hilft die Kontrollfrage: Wozu brauchen wir diese Daten?

Diesem Ziel kann auch eine Pseudonymisierung oder Anonymisierung von Daten dienen. Bei der **Pseudonymisierung** wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (in der Regel eine mehrstellige Buchstaben- oder Zahlenkombination, auch Hash genannt) ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren. Die **Anonymisierung** ist das Verändern personenbezogener Daten derart, dass diese Daten überhaupt nicht mehr einer Person zugeordnet werden können.

Soweit es der Rundfunkanstalt technisch möglich und zumutbar ist, hat sie die Nutzung ihrer Telemedienangebote anonym oder unter Pseudonym zu ermöglichen.

“Privacy by Design” und “Privacy by Default‘

Die Rundfunkanstalt sollte bereits in der Entstehungs- und Entwicklungsphase von Webseiten, Apps oder bei ihrer Präsenz auf Drittplattformen den datenschutzrechtlichen Vorgaben Rechnung tragen und durch datenschutzgerechte technische Gestaltung („Privacy by Design“) sowie datenschutzfreundliche Voreinstellungen („Privacy by Default“) dafür Sorge tragen, dass ihre Angebote datenschutzkonform sind. Der Datenschutz soll von vorneherein in die Gesamtkonzeption einbezogen werden anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturprogramme und anderem zu beheben. Dazu gehört auch, dass die Funktionalitäten standardmäßig datenschutzfreundlich voreingestellt sind.

Transparenz

Das Grundrecht auf informationelle Selbstbestimmung verlangt: Der Einzelne soll wissen, wer was wann und bei welcher Gelegenheit über ihn weiß. Das Transparenzprinzip wirkt sich an vielen Stellen im Datenschutzrecht aus:

Die Anbieter einer Webseite oder App sind insbesondere verpflichtet, die Nutzer in einer **Datenschutzerklärung** über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über eine etwaige Weitergabe der Daten an Dritte in einer leicht verständlichen Weise zu informieren (vergleiche hierzu die Hinweise zur Datenschutzerklärung).

Im Rahmen der **Einwilligung** muss dargestellt werden, welche Daten zu welchen Zwecken erhoben werden. Auch nach der Erhebung hat der Einzelne bestimmte **Nutzerrechte**: Jeder Nutzer, dessen personenbezogene Daten durch die Rundfunkanstalt erhoben und verwendet werden, hat das Recht, Auskunft über die zu seiner Person gespeicherten Daten zu verlangen. Unter bestimmten Voraussetzungen kann er zudem die Berichtigung, Löschung und Sperrung von Daten verlangen.

Datensicherheit

IT-Systeme sind aufgrund ihrer Komplexität anfällig für Fehler, über die zum Beispiel Unbefugte an Daten gelangen können. Gleichzeitig werden auch die Angriffe auf technische Systeme immer häufiger und ausgefeilter. Die Rundfunkanstalt hat daher gemeinsam mit dem IT-Sicherheitsbeauftragten und/oder der zuständigen Fachabteilung für ihre Webseiten und Apps geeignete

technische und organisatorische Maßnahmen zu ergreifen, um die Daten ihrer Nutzer gegen Verfälschung, Verlust und Missbrauch zu schützen.

Apps

Apps sind Applikationen, die an bestimmte Plattformen angepasst werden. Sie können als native und/oder hybride Apps zum Beispiel für mobile Endgeräte (Smartphone, Tablet) und stationäre Geräte (Smart-TV, Apple-TV und Ähnliches) angeboten werden. Sie können Daten in großem Umfang erfassen und verarbeiten, um dem App-Nutzer neue und innovative Dienstleistungen anzubieten. Viele Arten von Daten, die auf Endgeräten gespeichert sind oder von diesen Geräten erstellt werden, sind personenbezogene Daten und unterliegen damit datenschutzrechtlichen Regelungen.

Was sagt der Datenschutz?

Die größten Datenschutzrisiken für Nutzer sind die mangelnde Transparenz und die mangelnde Kenntnis der von einer App auf der jeweiligen Plattform ausgeführten Verarbeitung *personenbezogener* Daten sowie das Fehlen einer expliziten Einwilligung des Nutzers vor der Verarbeitung. Unzureichende Sicherheitsmaßnahmen, ein Trend zur Datenmaximierung und die ungenaue Festlegung der Zwecke, für die personenbezogene Daten erfasst werden, erhöhen die Risiken bei Apps zusätzlich.

Die Rundfunkanstalt ist datenschutzrechtlich für die von ihrer angebotenen App anfallenden Nutzerdaten vollumfänglich verantwortlich. Dies gilt auch dann, wenn die App über den Server eines Dienstleisters betrieben wird.

Die Verarbeitung von Nutzerdaten durch die App-Store-Betreiber bei der Anmeldung zum Store und dem Herunterladen einer App liegt dagegen außerhalb der Verantwortung der Rundfunkanstalt.

Checkliste

Als App-Anbieter und –Entwickler hat die Rundfunkanstalt für eine datenschutzkonforme App auf Folgendes zu achten.

Welche personenbezogenen Daten werden genutzt?

Apps und mobile Geräte enthalten bzw. erfassen Informationen, die auf den ersten Blick nicht immer als „personenbezogene Daten“ im Sinne des Datenschutzrechts zu erkennen sind. Die Bestimmbarkeit einer Person im Zusammenhang mit mobilen Geräten und Apps ist insbesondere bei folgenden Informationen zu bejahen:

\ IP-Adresse des Nutzers
\ Standortdaten
\ Kontakte
\ Eindeutige Geräte- und Kartenkennungen, Identität der betroffenen Person
\ Name des Telefons (Nutzer neigen dazu, ihr Telefon unter Verwendung ihres eigenen Namens zu benennen, zum Beispiel „Max Mustermanns iPhone“)
\ Kreditkarten- und Zahlungsdaten
\ Anruflisten, SMS oder Instant Messaging
\ Browserverlauf
\ E-Mail
\ Authentifizierungsdaten für spezielle Dienste, insb. Social Media
\ Foto- und Filmaufnahmen einer Person; Audiodaten mit Stimmaufnahmen

„Privacy by Design“/ „Privacy by Default“

Die Rundfunkanstalt sollte bereits in der Entstehungs- und Entwicklungsphase einer App den datenschutzrechtlichen Vorgaben Rechnung tragen und durch datenschutzgerechte technische Gestaltung („Privacy by Design“) sowie datenschutzfreundliche Voreinstellungen („Privacy by Default“) Sorge tragen. Aus diesem Grund ist bereits bei der Entwicklung einer App darauf zu achten, dass durch diese später nur diejenigen personenbezogenen Daten erhoben und verwendet werden, welche für die Durchführung der gewünschten Funktion unbedingt erforderlich sind.

Möglichkeit der anonymen und pseudonymen Nutzung

Soweit es möglich ist, sollte die Rundfunkanstalt die Nutzung ihrer App anonym oder unter Pseudonym ermöglichen. Über diese Möglichkeit ist der Nutzer zu informieren. Achtung: Eindeutige Geräte- und Kartenkennungen oder die IP-Adresse stellen kein Pseudonym dar!

Berechtigungen nur nach dem Grundsatz der Zweckbindung

Nach der Installation einer App müssen zur Erbringung des Dienstes in der Regel Berechtigungen bei dem Nutzer eingeholt werden, mittels derer die Rundfunkanstalt sowohl auf Funktionen des Gerätes als auch auf Daten, welche auf dem Gerät gespeichert sind, zugreifen kann.

Hier gilt: Es dürfen nur die für die App tatsächlich erforderlichen Berechtigungen vom Nutzer angefordert werden. Einige Betriebssysteme bieten Berechtigungen nur in festen Kombinationen an, welche neben der erforderlichen Berechtigung auch nicht nötige Berechtigungen

enthalten. Die Rundfunkanstalt muss in der Datenschutzerklärung über diesen Umstand aufklären und sich gegenüber dem Nutzer dazu verpflichten, von der nicht erforderlichen Berechtigung keinen Gebrauch zu machen.

Es gilt: Grundsatz der Einwilligung

Sollen personenbezogene Daten (zum Beispiel über entsprechende Formulare in der App) erhoben werden, so ist dazu grundsätzlich die ausdrückliche Einwilligung des Nutzers erforderlich (siehe hierzu die Hinweise zur Einwilligung in den Datenschutz „Basics“).

Erlaubt: Nutzung von Daten, die zur Inanspruchnahme der App notwendig sind

Ohne ausdrückliche Einwilligung darf die Rundfunkanstalt sogenannte Nutzungsdaten eines Nutzers erheben. Nutzungsdaten sind solche personenbezogenen Daten, welche notwendigerweise zur tatsächlichen Nutzung der App durch die Rundfunkanstalt erhoben und verwendet werden müssen (zum Beispiel die IP-Adresse oder – soweit im Einzelfall erforderlich – eindeutige Kennnummern).

Erlaubt: Pseudonyme Nutzungsprofile unter bestimmten Voraussetzungen

Grundsätzlich dürfen Nutzerdaten nur mit ausdrücklicher Einwilligung protokolliert werden. Aber: Zu Marktforschungszwecken (insbesondere Reichweitenmessung) können unter Beachtung bestimmter Voraussetzungen pseudonyme Nutzungsprofile erstellt werden.

Der Nutzer muss im Rahmen der Datenschutzerklärung auf die Erstellung des Nutzungsprofils und auf die Möglichkeit, der Erstellung zu widersprechen hingewiesen werden. Dazu muss ihm eine direkte Opt-Out Möglichkeit (Aus-Schalter in den App-Einstellungen) zur Verfügung gestellt werden, welche mit einem Klick aktiviert werden kann. Der bloße Hinweis auf bestimmte Einstellungsmöglichkeiten am Gerät etc. genügt nicht. Widerspricht der Betroffene der Profilbildung unter Pseudonym, so sind etwa vorhandene Profildaten zu löschen oder wirksam zu anonymisieren (siehe hierzu die Hinweise zur Web-Analyse).

Push-Funktionen mit Zustimmung des Nutzers zulässig

Mit der Push-Funktion können verschiedene Inhalte – zum Beispiel Kurznachrichten, Live-Ticker und so weiter – von einem Server zu einem speziellen Mobilgerät versandt werden. Hat der Nutzer einmal den Dienst abonniert, übernimmt der Server eigeninitiativ das „Pushen“ des Inhalts zum Nutzer-Device.

Damit die Rundfunkanstalt weiß, wer welche Push-Nachrichten möchte, ist eine eindeutige Kennung erforderlich. Es wird empfohlen, keine personenbezogene Nutzerdaten zu erheben, sondern mit einer zufallsgenerierten eindeutigen Nummer (sogenannte Token oder Device Token ID) zu arbeiten: Mit Zustimmung des Nutzers wird durch das Betriebssystem des Gerätes des Abonnenten ein Token generiert. Die Device Token ID wird an den Server übermittelt. So weiß die Rundfunkanstalt, an wen sie welche Push-Nachrichten schicken muss. Durch solche zufallsgenerierte Token wird die Möglichkeit der App-übergreifenden Nachverfolgung von Nutzern eingeschränkt.

Auf die Funktionalität der Device Token ID ist in der Datenschutzerklärung hinzuweisen.

Achtung bei Standortdaten

Sofern durch die App auf Standortdaten des Geräts zugegriffen wird, muss darauf geachtet werden, dass dies nur im zulässigen Umfang geschieht. Hier sind die Hinweise zu Standortdaten zu beachten.

Achtung beim Einbinden von Inhalten von Drittanbietern

Werden Inhalte von Drittanbietern in die App eingebunden, besteht die Gefahr, dass allein durch das Aktivieren der App Nutzerdaten ohne Wissen und Wollen des jeweiligen Nutzers an die Drittanbieter fließen.

Hier muss auf eine datenschutzkonforme Gestaltung geachtet werden. Mit Hilfe von Vorschaltseiten kann zum Beispiel sichergestellt werden, dass die Nutzerdaten erst dann zu den Anbietern der eingebundenen Inhalte fließen, wenn der Nutzer zuvor entsprechend informiert worden ist im Rahmen der aus Datenschutzsicht gebotenen Zwei-Klick-Lösung (siehe hierzu die Hinweise zum Embedding von fremden Inhalten).

Umfassende spezifische Datenschutzerklärung vor Installation der App

Neben der Veröffentlichung eines Impressums hat die Rundfunkanstalt in einer eigenen Datenschutzerklärung in der App über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung der Nutzerdaten zu informieren. Was die wesentlichen Inhalte der Datenschutzerklärung sind, bestimmt sich anhand des Funktionsumfangs der App.

Wegen der beschränkten Display-Größe mobiler Endgeräte sind die Datenschutzhinweise so zu gestalten, dass der Nutzer jederzeit ohne großen Aufwand die gewünschten Informationen erhalten kann.

Eine einfache Verknüpfung mit der Datenschutzerklärung eines ähnlichen oder alternativen Webangebotes der Rundfunkanstalt genügt dann nicht, wenn es hinsichtlich der Datenverarbeitung relevante Unterschiede bei der Datenverarbeitung einer Webseite und einer App gibt.

Die App-spezifische Datenschutzerklärung muss **vor** der Installation der App erfolgen. Die Datenschutzerklärung muss also entweder im App-Store als Link oder nach dem Herunterladen für den Nutzer zum Abruf bereitgehalten werden.

Um dem Nutzer die unkomplizierte Wahrnehmung seiner Nutzerrechte zu ermöglichen, ist eine einfache Kontaktmöglichkeit zum Datenschutzbeauftragten anzugeben.

Auf Datensicherheit achten

Eine zentrale Rolle bei der datenschutzgerechten Gestaltung spielt die Sicherheit einer App. Insbesondere an folgendes ist zu denken:

/ Sowohl beim Versand als auch beim Empfang von Daten zwischen Nutzer und Rundfunkanstalt sollte die Kommunikationsverbindung mit dem Backend durch eine Transportverschlüsselung abgesichert sein.

/ Es sollten nur diejenigen personenbezogenen Daten lokal auf dem Gerät gespeichert werden, die unbedingt für den Betrieb der App notwendig sind. Auch die Speicherdauer muss sich an dieser Notwendigkeit orientieren. Bei einer Deinstallation der App muss sichergestellt werden, dass die lokal gespeicherten personenbezogenen Daten des Nutzers sowie die Cookies gelöscht werden.

/ Sofern für das Nutzen der App eine eindeutige Kennung erforderlich sein sollte, wird empfohlen, eine zufallsgenerierte eindeutige Nummer (ein Token) zu erzeugen, die im Rahmen der App-Nutzung zwar eindeutig ist, außerhalb der App oder bei Neuinstallation jedoch keinen Bezug mehr zum Gerät bzw. Nutzer ermöglicht.

Achtung bei Beauftragung von Dritten

Die Rundfunkanstalt ist datenschutzrechtlich vollumfänglich verantwortlich, wenn sie eine App anbietet. Dies gilt auch dann, wenn die App im Auftrag der Rundfunkanstalt von Dienstleistern entwickelt, programmiert oder gehostet wird oder sonstige Daten (zum Beispiel Device Token ID) durch einen externen Dienstleister verarbeitet werden

Falls ein Dritter mit der Entwicklung der App beauftragt ist, ist darauf zu achten, dass keine personenbezogenen Daten übertragen werden. Eine Erhebung und Verwendung personenbezogener Daten des Nutzers einer App ist auf Entwicklerseite in der Regel nicht erforderlich und müsste deshalb im Einzelfall begründet werden und von einem Erlaubnistatbestand gedeckt sein.

Im Übrigen gelten die Hinweise zur Auftragsvergabe an Dritte.

Minderjährigen-Datenschutz

Bei Apps speziell für Kinder und Jugendliche sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Auftragsvergabe an Dritte

Vergibt eine Redaktion oder der für Web-Technik zuständige Fachbereich Aufträge an Dritte – zum Beispiel für App-Programmierung oder das Programmieren von anderen Anwendungen, Hosting, Medienforschung und so weiter – und erhält beziehungsweise verarbeitet dieser externe Dienstleister dabei personenbezogene Daten der Nutzer, müssen die gesetzlichen und hausinternen Regelungen zur Datenverarbeitung durch Dritte beachtet werden. In diesem Kontext gewinnen zunehmend auch „Cloud-Dienste“, die von externen Unternehmen angeboten werden, an Bedeutung.

Was sagt der Datenschutz?

Vorab ist gemeinsam mit dem Datenschutzbeauftragten zu klären, ob es sich um eine sogenannte Auftragsdatenverarbeitung im Sinne des Datenschutzrechts handelt.

Auftragsdatenverarbeitung (ADV) ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen externen Dienstleister **im Auftrag** der verantwortlichen Stelle – also der jeweiligen Rundfunkanstalt. In diesem Fall bleibt ausschließlich die Rundfunkanstalt für die Verarbeitung der Daten verantwortlich. Die Rundfunkanstalt hat die Zulässigkeit der Datenverarbeitung zu prüfen, die Erfüllung der Nutzerrechte zu gewährleisten und mögliche Haftungsrisiken zu tragen. Es gibt detaillierte gesetzliche Vorgaben, welche Rechte, Pflichten und Maßnahmen in diesem Fall durch eine gesonderte schriftliche Vereinbarung zwischen dem Auftraggeber (also der Rundfunkanstalt) und dem Dienstleister zu treffen sind. Ganz wesentlich ist dabei die Datensicherheit: Das Schutzniveau für die Daten muss mindestens dem Schutzniveau bei Abwicklung im eigenen Unternehmen entsprechen.

Checkliste

Grundsätzlich: Bevorzugung einer „Inhouse“-Lösung

Eine Vergabe von Aufträgen an Externe ist grundsätzlich möglich. Die hohen datenschutzrechtlichen Maßstäbe für öffentlich-rechtliche Angebote können aber regelmäßig am besten durch die Rundfunkanstalt selbst realisiert und kontrolliert werden. Sofern möglich, sollten die jeweiligen Nutzerdaten daher **in** der Rundfunkanstalt verarbeitet und gespeichert werden (zum Beispiel Inhouse-Programmierung und dem Hosten der App auf anstaltseigenen Servern). Eine Durchführung durch externe Dritte sollte gegenüber einer anstaltsinternen Lösung nur nach Abwägung aller relevanten Aspekte bevorzugt werden.

Vor Auftragsvergabe: Sind personenbezogene Daten betroffen?

Es ist vorab zu klären, ob der Dienstleister im Zusammenhang mit seinem Auftrag personenbezogene Daten von Nutzern erhält bzw. verarbeitet. Nur dann gelten die datenschutzrechtlichen Regelungen zur ADV. Die Einordnung ist nicht immer einfach. Sofern ein Auftrag an Dritte erfolgen soll, bei dem möglicherweise Nutzerdaten übermittelt werden, sollte im Zweifel die zuständige Beschaffungsstelle (zum Beispiel der Einkauf), die IT-Sicherheit und/oder der Datenschutzbeauftragten eingebunden werden.

Bei Auftragsdatenverarbeitung: Beachtung der anstaltsinternen Regelwerke

Sofern es sich um eine ADV handelt, sind die einschlägigen hausinternen Regelungen zu beachten. In einigen Rundfunkanstalten gibt es entsprechende Dienstanweisungen zur ADV oder formalisierte Abläufe und Mustertexte für die erforderliche Vereinbarung. In allen Fällen können die Beschaffungsstellen und der Datenschutzbeauftragte weiterhelfen.

Hierauf ist besonders zu achten!

Einige Dienstleister arbeiten auch für private Anbieter und sind sich der besonders hohen datenschutzrechtlichen Standards für die Angebote der Rundanstalten nicht immer bewusst. Oftmals ist für externe Dienstleister zum Beispiel die Datenspeicherung außerhalb der EU üblich oder Dienstleister mit Sitz außerhalb der EU können auf Daten *innerhalb* der EU zugreifen. Für die Übermittlung/Verarbeitung von Daten in sogenannte Drittländer – das heißt Staaten außerhalb der EU – gelten besonders hohe Zulässigkeitsanforderungen; zudem sind zusätzliche datenschutzrechtliche Absicherungen erforderlich.

Einige Dienstleister implementieren für ihre kommerziellen Auftraggeber oder die eigenen Zwecke regelmäßig Tracking-Tools. Deshalb ist es wichtig, dass die Rundfunkanstalt die eigenen Anforderungen klar definiert und kommuniziert.

Es ist zu empfehlen, jede beauftragte Anwendung vor dem Ersteinsatz und nach Updates daraufhin zu testen, ob nicht doch – versehentlich und unbedacht – datenschutzrechtlich problematische Applikationen implementiert sind, die Daten an andere Dritte (zum Beispiel Google oder Facebook und so weiter) übermitteln. Dies gilt auch dann, wenn der Auftrag selbst – zum Beispiel die App-Programmierung – eigentlich nicht als ADV einzuordnen ist.

Information über Verarbeitung von Nutzerdaten durch Dritte

Aus Gründen der Transparenz kann in der Datenschutzerklärung darüber informiert werden, dass die Rundfunkanstalt bei bestimmten Projekten durch Dritte unterstützt wird und dabei Nutzerdaten durch Dritte gespeichert oder verarbeitet werden.

Bei einer Erhebung und Nutzung von Nutzerdaten durch Dienstleister mit Sitz in einem Drittstaat außerhalb der EU/EWR und/oder mit Zugriff auf die Daten aus Drittstaaten *muss* hierüber in der Datenschutzerklärung informiert werden.

Chats, Foren, Gästebücher, Kommentarfunktionen

Kommentarfunktionen, Chats und andere interaktive Tools zum Austausch der Nutzer untereinander und zum Veröffentlichen eigener Inhalte wie zum Beispiel Fotos oder Videos (sogenannte User Generated Content) sind mittlerweile gängiger Bestandteil öffentlich-rechtlicher Online-Angebote. Um sicherzustellen, dass diese Tools datenschutzkonform eingesetzt werden und der Austausch mit den Nutzern konstruktiv und angenehm bleibt, bedarf es klarer Regelungen und redaktioneller Begleitung.

Was sagt der Datenschutz?

Wer auf seiner Webseite Chats, Foren und andere interaktive Funktionen anbietet, verarbeitet Daten und Inhalte seiner Nutzer. In den meisten dieser Fälle müssen sich die Besucher registrieren oder zumindest eine E-Mail-Adresse angeben. Dadurch entsteht ein datenschutzrechtlich relevanter „Personenbezug“. Interaktive Tools können aber auch so eingerichtet werden, dass jeder Besucher einen Beitrag ohne weitere Angaben veröffentlichen kann. Dabei ist aber zu bedenken, dass

auch der Inhalt eines (vermeintlich) anonymen Beitrags einen Personenbezug im rechtlichen Sinne aufweisen kann. Rechtlich macht es daher fast keinen Unterschied, ob Nutzer sich registrieren müssen oder auch ohne weitere Angaben mitmachen können.

Die Kommentare der Nutzer können u.a. das Recht Dritter auf informationelle Selbstbestimmung verletzen: Das kann dann der Fall sein, wenn personenbezogene Daten wie Anschriften, E-Mail-Adressen und Telefonnummern in den Kommentaren veröffentlicht werden. Gleiches gilt für offenkundig private Korrespondenz, wie Briefe, E-Mails und Ähnliches

Checkliste

Datenschutzrechtlich erforderliche Einwilligung des Nutzers

Es empfiehlt sich, für die Teilnahme an Chats, Foren unter anderem eine aktive Einwilligung des Nutzers einzuholen (zum Beispiel durch aktives Setzen eines Häkchens in der Checkbox). In der Regel fallen folgende Angaben an:

\ die Beiträge der Nutzer selber,
\ hinzu kommt in aller Regel ein Nutzername und oft auch ein Passwort sowie eine E-Mail-Adresse
\ auch bei einfachen Internetseiten fallen die Daten des HTTP-Requests an:
IP-Adresse, Zeit des Zugriffs und andere Angaben

Bei einer Registrierung für Chats unter anderem oder dem Beitritt zu einem Forum gilt grundsätzlich: Es sollen nur so viele personenbezogene Daten des Nutzers wie unbedingt nötig abfragt werden und diese Daten dürfen nur für den konkreten Zweck (Zugang zum Forum und so weiter) gespeichert und genutzt werden. Eine Double-Opt-In-Lösung zur Nutzerregistrierung ist empfehlenswert. Bei der Registrierung sollte zudem vorgesehen sein, dass sich der Nutzer einen Nickname wählen kann, damit so auf die Veröffentlichung des Klarnamens verzichtet werden kann.

Es ist nützlich, bei der Einwilligungserklärung die wichtigsten Informationen kompakt zusammenzufassen. Die Details können dann mit einem weiteren Klick – zum Beispiel in der allgemeinen Datenschutzerklärung – verfügbar gemacht werden. Auch auf die Nutzungsbedingungen (siehe unten) kann verlinkt werden.

Die Nutzer sind berechtigt, ihre Einwilligung zur Speicherung der Daten jederzeit schriftlich mit Wirkung für die Zukunft zu widerrufen. In einem solchen Fall ist der entsprechende Zugang zu löschen.

Nutzungsbedingungen und Netiquette

Die Rundfunkanstalten haben in Nutzungsbedingungen und Netiquette die Rahmenbedingungen festzulegen, die von Nutzern vor ihrer Teilnahme an Chats, Foren und Ähnliches zu akzeptieren sind. Dort soll unter anderem auch definiert sein, welche Form der Kommunikation erwünscht ist, was verboten ist und wie bei Verstößen vorzugehen ist.

Beispiele hierfür sind:

„Netiquette“ auf ARD.de:
http://www.ard.de/home/ard/ARD_de_Netiquette/119854/index.html

Nutzungsbedingungen für die Community bei DasErste.de: http://www.daserste.de/specials/service/nutzungsbedingungen100.html

Richtlinien auf tagesschau.de:
https://meta.tagesschau.de/richtlinien

Die Netiquette beziehungweise die Nutzungsbedingungen sollten – wie die Einwilligung auch – durch den Nutzer aktiv bestätigt werden (zum Beispiel via Checkbox). Die Nutzungsbedingungen können einen eigenen Passus zum Datenschutz enthalten oder es kann auf die allgemeine Datenschutzerklärung des Onlineangebotes verlinkt werden.

Löschung von persönlichen Nutzerdaten – Löschung von Inhalten

Persönliche Daten der Nutzer sind zu löschen, sobald sie nicht mehr erforderlich sind. Dies ist der Fall bei Abmeldung des Nutzers oder bei Widerruf der Einwilligung zur Speicherung der Daten. Dem Nutzer sollte zudem selbst die Möglichkeit eingeräumt werden, seinen Account zu löschen (seine Kommentare können dann neutral „Gast“ zugewiesen werden)

Wenn die **Inhalte** der Kommentare nicht den Vorgaben der Netiquette und der Nutzungsbedingungen entsprechen, können sie gelöscht und/oder der Nutzer gesperrt werden. Dies ist unter anderem dann von Bedeutung, wenn Dritte durch die Veröffentlichung in ihrem Recht auf informationelle Selbstbestimmung verletzt sind.

Auf Datensicherheit achten

Aus dem Prinzip der Datensicherheit folgt, dass man geeignete Sicherheitsmaßnahmen natürlich insbesondere für die Passwörter vorsieht. Aber auch die anderen Daten sind fachgerecht vor unbefugten Zugriffen zu sichern.

Achtung bei der Verwendung von Nutzernamen

Die in den Chats, Foren und Ähnliches genutzten Namen sind nicht immer die Klarnamen der tatsächlich handelnden Nutzer. Hier können falsche Eindrücke entstehen, wenn Personen bestimmte Äußerungen zugeschrieben werden, ohne dass sie tatsächlich die Quelle sind. Es sollte nicht vorschnell geurteilt, sondern auch hier gewissenhaft recherchiert werden.

Achtung bei Angeboten für Minderjährige

Bei Angeboten für Minderjährige sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Auf sonstige rechtliche Aspekte achten

Bei von Nutzern eingestellten Inhalten (Kommentare, User Generated Content) sind regelmäßig weitere rechtliche Aspekte zu beachten (zum Beispiel Urheberrecht, Persönlichkeitsrecht). Hierzu ist Rücksprache mit dem zuständigen Justitiariat zu halten.

Cookies

Fast alle Webseiten speichern Cookies auf Geräten (PC, Handy etc.) eines Benutzers, um eine optimale Kommunikation zwischen der Website und dem Browser des Benutzers sicherzustellen. Cookies sind kleine Textdateien, die lokal im temporären Speicher des Internet-Browsers eines Seitenbesuchers gespeichert werden. Sie sind dazu da, den Nutzer wiederzuerkennen und ihm das Surfen auf einer Website zu erleichtern, etwa dadurch, dass der Nutzer seine Zugangsdaten nicht bei jedem Besuch neu eingeben muss. Cookies ermöglichen es aber auch, ein komplexes Nutzungs- und Surfverhalten zu ermitteln.

Es gibt unterschiedliche Arten von Cookies: Cookies können nach ihrer Lebensdauer unterschieden werden – Session Cookie oder permanente Cookie – und danach, zu welchem Anbieter sie gehören – dem Anbieter der Webseite selbst oder einem Drittanbieter, der mit der Webseite verbunden ist.

Session Cookies (temporäre Cookies)

Sie werden eingesetzt, um einen Benutzer wiederzuerkennen, der auf dieser Website gesurft ist oder um zu erkennen, ob ein Benutzer bereits eingeloggt ist. Sitzungscookies werden automatisch gelöscht, wenn der Benutzer den Browser schließt.

Permanente Cookies (dauerhaft gespeicherte Cookies)

Diese werden auf dem Computer eines Benutzers gespeichert und laufen entweder zu einem bestimmten Datum/innerhalb eines vorgegebenen Zeitrahmens ab oder haben überhaupt kein Ablaufdatum.

Was sagt der Datenschutz?

Cookies sind datenschutzrechtlich relevant, wenn sie über enthaltene Informationen wie etwa Benutzernamen oder IP-Adresse einen Personenbezug herstellen.

Unproblematisch: Für die Nutzung einer Seite unbedingt erforderliche Cookies

Cookies, die für die aktuelle Nutzung der Seite zwingend erforderlich sind, weil ohne sie ein Onlinedienst technisch gar nicht funktionieren würde, sind datenschutzrechtlich unproblematisch. Dazu gehören zum Beispiel Cookies, die mehrseitige Formulare speichern. Auch geht es hier um Informationen über die Spracheinstellungen oder um Login-Daten für die jeweilige Sitzung (Cookies zur Verbesserung der Funktionalität oder der Leistung/Performance der Webseite). Regelmäßig handelt es sich hierbei um temporäre Cookies, die nach der Nutzung wieder gelöscht werden.

Achtung bei optionalen Cookies für zusätzliche Zwecke

Bei optionalen Cookies für zusätzliche Zwecke ist die Rechtslage unklar und umstritten. Das trifft insbesondere zu auf Analyse- und Tracking-Cookies, die die Verfolgung des Nutzerverhaltens im Internet ermöglichen. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. Ebenso betrifft dies Cookies von Social-Media-Plattformen wie Facebook.

Das deutsche Recht kennt aktuell keine direkte Pflicht, die Nutzer in die Verwendung von Cookies einwilligen zu lassen. Danach ist es ausreichend, den Nutzer über den Einsatz dieser optionalen Cookies in der Datenschutzerklärung zu unterrichten und auf ein Widerspruchsrecht hinzuweisen (sogenannte „Opt-out“-Verfahren). Die einschlägigen europäischen Regelungen fordern dagegen grundsätzlich die aktive Einwilligung des Nutzers nach vorher erfolgter umfangreicher Aufklärung (sogenannte „Opt-in“-Verfahren).

Checkliste

Praxis: Informationen in der Datenschutzerklärung und „Opt-out“-Verfahren

Angesichts der unklaren Rechtslage besteht derzeit eine Option darin, bis auf weiteres das „Opt-out“-Verfahren zu praktizieren und abzuwarten, wie sich die deutsche Rechtslage hier möglicherweise ändert. In

diesem Fall hat die Rundfunkanstalt über den Einsatz von Cookies umfassend in der Datenschutzerklärung zu informieren und den Nutzer auf sein Widerspruchsrecht beim Einsatz von Cookies und bei der Bildung von Nutzungsprofilen hinzuweisen. Zudem ist dem Nutzer zu erklären, wie er das Setzen von Cookies verhindern bzw. diese durch Einstellungen in seinem Browser löschen kann.

Bei Webanalyse-Tools sollte dem Nutzer auch unmittelbar eine technische Möglichkeit zum Widerspruch eingeräumt werden. In der Regel kann durch Anklicken eines entsprechenden Links das jeweilige Cookie deaktiviert werden (siehe hierzu die Hinweise zur Web-Analyse).

Rechtlich sicherste Variante: Informationen auf Startseite und „Opt-in“-Verfahren

Angesichts der unklaren rechtlichen Situation ist die sicherste Variante, wenn die Rundfunkanstalt die vorherige **Einwilligung** des Nutzers einholt. Es sind hierzu sichtbare Informationen auf der Startseite zu hinterlegen, denen der Nutzer wissentlich und aktiv zustimmen kann, und zwar dies *bevor* das erste Cookie auf dessen Endgerät gelangt. Der Einwilligungstext sollte beim ersten Aufruf der Seite eingeblendet werden. Der Text sollte so konkret wie möglich sagen, um welche Daten es geht, wozu diese genutzt werden und an wen diese Daten weiter gegeben werden. Der Nutzer muss diesen Text mit einem Klick bestätigen. Diese Einwilligung ist zu protokollieren und vorzuhalten im Falle von Nachfragen.

Wichtig: Ein Pop-up-Fenster ist ungenügend, weil dieses unter Umständen nutzerseitig geblockt werden könnte. Daher greifen fast alle Seitenbetreiber zu sogenannte Lay-Over-Ein-blendungen am oberen oder unteren Rand des Bildschirms.

Die angezeigten Informationen müssen einen kurzen allgemeinen Hinweis über Cookies und einen Link zu detaillierteren Informationen (in der Regel zur Datenschutzerklärung, alternativ zu einer eigenen Cookie-Informationsseite) enthalten. Zudem muss ein klickbarer Button zur Einwilligung vorhanden sein. Hierbei darf es sich nicht um einen voreingestellten Zustimmungsbutton („gesetztes Häkchen") handeln – dem Nutzer muss die Wahl zwischen Zustimmung und Ablehnung gegeben werden. Und: Eine Ablehnung eines solchen optionalen Cookie darf die Nutzung der Seite nicht beeinträchtigen.

Im Fall einer Nutzerbeschwerde ist der Seitenbetreiber in der Beweispflicht – er muss beweisen, dass der entsprechende Nutzer seine Einwilligung in die Verwendung von Cookies gegeben hat. Allgemeine Texte wie "*Durch die weitere Nutzung dieser Webseite erklären Sie sich mit der Verwendung von Cookies einverstanden*" sind rechtlich nicht sicher.

Die EU-Kommission bietet für Webseitenanbieter ein Tool – ein sogenannte Cookie Consent Kit – zur rechtskonformen Umsetzung für den Einsatz von Cookies an (siehe hierzu unter: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm).

In jedem Fall: Information zum Einsatz von Cookies in der Datenschutzerklärung!

Wichtig. In **allen** Varianten hat die Rundfunkanstalt in der Datenschutzerklärung einen entsprechenden Passus zu Cookies und Hinweise für den Nutzer aufzunehmen, wie er das Setzen von Cookies verhindern kann. Es muss eindeutig, leicht auffindbar und in verständlicher Sprache aufgeführt werden,

- was genau in den Cookies gespeichert wird; dabei ist je nach Cookie zu differenzieren,
- zu welchem Zweck gespeichert wird,
- wie lange gespeichert wird,
- wer genau für die Speicherung verantwortlich ist sowie
- dass und wie der Nutzer von seinem Widerrufsrecht Gebrauch machen kann.

Achtung bei Angeboten für Minderjährige

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Datenschutzerklärung

Webseiten und Apps sammeln inzwischen eine Vielzahl an Daten über ihre Nutzer, die dem Datenschutz unterliegen. Eine Datenschutzerklärung eines Onlineangebots oder einer App ist daher unerlässlich, um die Datensouveränität der Nutzer zu wahren und Vertrauen zwischen Rundfunkanstalt und Nutzer zu schaffen. Sie sollen dem Besucher einer Webseite transparent und verständlich aufzeigen, was häufig von ihm unbemerkt und im Hintergrund mit seinen persönlichen Daten passiert.

Was sagt der Datenschutz?

Das Datenschutzrecht **verpflichtet** die Rundfunkanstalten, die Nutzer ihres Onlineangebotes über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten sowie über eine etwaige Weitergabe der Daten an Dritte allgemein in einer leicht verständlichen, lesbaren Weise zu informieren.

Eine Datenschutzerklärung ist strikt zu unterscheiden

\ von einer datenschutzrechtlichen **Einwilligung**:
In der Datenschutzerklärung erläutert die Rundfunkanstalt rein informierend, was sie mit den Daten (aufgrund gesetzlicher Befugnisse) unternimmt. Bei einer datenschutzrechtlich relevanten Einwilligung holt die Rundfunkanstalt eine explizite Zustimmung des Nutzers ein, um die Daten in einer Art und Weise zu nutzen, die das Gesetz nicht per se erlaubt.

\ vom **Impressum** einer Webseite:
Ein Impressum – manchmal auch „Anbieterkennzeichnung“ genannt – ist in der Regel gesetzlich erforderlich für Veranstalter einer Webseite. Dabei handelt es sich um eine allgemeine medienrechtliche Pflicht: Besucher einer Webseite sollen wissen können, mit wem sie es zu tun haben. Das dient allerdings auch dem datenschutzrechtlichen Prinzip der Transparenz. Der Link oder Reiter auf das Impressum sollte als solcher benannt werden. Von jeder Unterseite aus sollte der Nutzer mit einem Klick herausfinden können, wer Veranstalter des Angebots ist.

Checkliste

Form: Allgemein verständlich, leicht auffindbar und jederzeit abrufbar

Die Datenschutzerklärung sollte in allgemein verständlicher, lesbarer Form formuliert sein. Technische oder juristische Fachbegriffe und Formulierungen sind daher zu vermeiden.

Bereits auf der Startseite muss ein eindeutiger, leicht auffindbarer Hinweis auf diese Informationen zu finden sein. Zudem müssen sie jederzeit abrufbar sein. Die Datenschutzerklärung sollte daher auf der Internetseite unter einem eigenen Menüpunkt „Datenschutzerklärung“ oder „Datenschutzhinweis“ als Link eingebunden und von jeder Seite und Unterseite aus erreichbar sein. Bei Änderungen ist der Inhalt zu aktualisieren.

Bei Telemedienangeboten für Minderjährige ist zusätzlich eine verständliche Form für Kinder und Jugendliche erforderlich (siehe hierzu die Hinweise zum Minderjährigen-Datenschutz).

Inhalt: Was muss alles drin sein?

Eine Datenschutzerklärung muss grundsätzlich für das gesamte Onlineangebot formuliert werden. Die Angaben, die zu machen sind, richten sich nach den spezifischen Angeboten und Funktionen der Seite.

Grundsätzlich gilt es, die Nutzer der Seite über die Art, den Umfang und die Zwecke der Erhebung und die Verwendung personenbezogener Daten zu unterrichten. Je mehr Daten von den Nutzern erhoben werden und je sensibler die Daten sind, desto ausführlicher muss die Unterrichtung sein. Ebenfalls zu benennen sind eventuelle Weitergaben der Daten in Länder außerhalb der EU.

Informationen darüber, welche personenbezogenen Daten des Nutzers erfasst werden

Bei Aufruf und Nutzung der Seite oder App

Server-Log-Daten (Datum und Uhrzeit des Besuches, die verwendete IP-Adresse, Browsertyp/-version und Betriebssystem; besuchte Webseiten und Herkunftsseite); Gerätedaten; Standortdaten oder ähnliches.

Aufgrund der Anmeldung (Registrierung)

Name; Geschlecht; Geburtsdatum; Anschrift; Kontaktdaten (Mail, Telefonnummern), Fotos, Standortdaten oder ähnliches.

Aufgrund sonstiger Funktionen, insb. Anwendungen von externen Dienste-Anbietern

Gewinnspiele; Nutzerforen; Kommentarfunktionen; Newsletter-Abonnements; Kontaktformulare; Webanalysen; Social-Media-Funktionen; Tools von sonstigen externen Diensten und Drittplattformen oder ähnliches.

Informationen darüber, auf welche Weise und für welchen Zweck die Daten erhoben und genutzt werden

Cookies und Plug-Ins

Welche Cookies oder Plug-ins werden genutzt, welche Daten werden dabei wozu durch die Rundfunkanstalt oder Dritte genutzt?

Tracking-Tools

Welche Tracking-Dienste werden eingesetzt, welche Tracking-Daten werden wozu genutzt?

Zugriffsrechte (bei Apps)

Auf welche Daten wird zugegriffen? Weshalb erfolgt wann wozu ein Zugriff?

Eingaben des Nutzers

Welche Daten stammen für welchen Zweck von Eingaben des Nutzers selbst?

Einwilligung

Es ist transparent zu machen, welche Datenerhebungen und-verarbeitungen zu welchem Zweck von der Einwilligung des Nutzers abhängen.

Information über Nutzerrechte

Widerruf der Einwilligung

Der Nutzer ist auf die Möglichkeit des Widerrufs einer erteilten Einwilligung hinzuweisen, inklusive einer einfachen Kontaktmöglichkeit (zum Beispiel per E-Mail).

Anonyme/pseudonyme Nutzung

Der Nutzer ist über die Möglichkeit zu informieren, das Onlineangebot anonym oder unter Pseudonym nutzen zu können

Widerspruchsrecht bei Cookies, pseudonymen Nutzungsprofilen

Der Nutzer ist auf sein Widerspruchsrecht beim Einsatz von Cookies und bei der Bildung von Nutzungsprofilen hinzuweisen (siehe die Hinweise zur Web-Analyse).

Nennung eines Ansprechpartners

Am Ende der Datenschutzerklärung sollte ein Ansprechpartner für datenschutzrechtliche Anfragen und Beschwerden genannt werden (zum Beispiel der anstaltseigene Datenschutzbeauftragte). Dabei sollte eine einfache Möglichkeit der Kontaktaufnahme (zum Beispiel via E-Mail und Telefon) angeboten werden.

Hinweis auf Drittplattformen, auf denen die Rundfunkanstalt präsent ist

Aus Gründen der Transparenz sollte die Rundfunkanstalt in ihrer Datenschutzklärung auch informieren, dass sie mit eigenen Auftritten auf Social Media-Plattformen und anderen Drittplattformen präsent ist. Dem Nutzer sollte erklärt werden, welche Datenschutzrichtlinie für die Nutzung der jeweiligen Drittplattformen gilt (verbunden mit der Bitte an den Nutzer, diese aufmerksam zu lesen).

Drittplattformen

Die Rundfunkanstalten sind mit ihren Angeboten und Inhalten auf verschiedenen Drittplattformen präsent. Neben den Social Media Plattformen wie Facebook, Twitter und Google+ sind die Anstalten zum Beispiel auf der Videoplattform YouTube, auf Foto-/Content-Plattformen wie Instagram und Pinterest oder Streaming-Diensten wie Spotify vertreten. Daneben gibt es noch eine Vielzahl von anderen Drittplattformen, die von den Rundfunkanstalten im Hinblick auf ihre publizistische Bedeutung getestet oder zeitweise genutzt werden.

Was sagt der Datenschutz?

Drittplattformen – insbesondere soziale Netzwerke wie Facebook und andere – sind aus datenschutzrechtlicher Sicht sehr problematisch. Es ist davon auszugehen, dass diese Plattformen aus verschiedenen Gründen regelmäßig nicht den deutschen Datenschutzstandards entsprechen. Bedenken bestehen insbesondere in Bezug auf die Anforderungen an Transparenz, Datensparsamkeit und wirksame Einwilligung. Die meisten Drittplattformanbieter speichern die Daten zudem häufig außerhalb der EU in Ländern wie den USA, die kein vergleichbares Niveau an Datenschutz gewährleisten.

Aber: Im Hinblick auf die Präsenz von Rundfunkanstalten auf Drittplattformen ist grundsätzlich davon auszugehen, dass der jeweilige Plattformanbieter datenschutzrechtlich verantwortlich bleibt. Eine eigene datenschutzrechtliche Verantwortlichkeit trifft die Rundfunkanstalten bei der Nutzung dieser Plattformen nach geltendem Recht nicht.

Unabhängig von der formalrechtlichen Verantwortlichkeit sollte die Rundfunkanstalt ihre Präsenz auf Drittplattformen so datenschutzgerecht wie möglich ausgestalten.

Checkliste

Überprüfung der Datenschutzrichtlinien / AGB der Drittplattform – Check des publizistischen Mehrwerts

Sofern die Rundfunkanstalt auf einer Drittplattform präsent sein will, sollten vorab die Datenschutzrichtlinien sowie die sonstigen AGB oder Nutzungsbedingungen des Drittanbieters geprüft werden. Oftmals enthalten diese AGB für die Rundfunkanstalt problematische urheberrechtliche und sonstigen Klauseln. Möglicherweise lässt sich der jeweilige Anbieter im Rahmen einer eigenen Vereinbarung mit allen Rundfunkanstalten zur Einhaltung der deutschen Standards bewegen.

Regelmäßig weisen Drittplattformen die bekannten Datenschutzmängel auf, die die Nutzer dieser Angebote treffen können. Insofern sollte gewissenhaft abgewogen werden, ob der publizistische Mehrwert trotzdem für die Präsenz der Rundfunkanstalt auf dieser Plattform spricht. Dieser Check sollte regelmäßig wiederholt werden.

Datenschutzkonformes Verhalten der Rundfunkanstalt auf Drittplattformen

Unabhängig von der formalrechtlichen Verantwortlichkeit sollte die Rundfunkanstalt ihre Präsenz auf Drittplattformen so datenschutzgerecht wie möglich ausgestalten.

Dies bedeutet zum Beispiel, dass die Rundfunkanstalten die Nutzer nicht dazu einladen dürfen, sensible Informationen (zum Beispiel im Rahmen von Upload-Aktionen) preiszugeben.

Auch Datenflüsse zwischen Drittplattform und Rundfunkanstalt ohne Wissen und Wollen des Nutzers sind zu verhindern (siehe hierzu auch die Hinweise zum Embedding von fremden Inhalten).

Machen Nutzer von ihren Rechten (Recht auf Auskunft, Berichtigung oder Löschung) Gebrauch, sollte die Rundfunkanstalt – soweit technisch möglich und vom Aufwand her zumutbar – diese Daten selbst zu löschen bzw. zu sperren. Eine Verweisung des Nutzers an den Plattformbetreiber sollte erst im zweiten Schritt für die Maßnahmen erfolgen, die nur durch den Plattformanbieter selbst zu realisieren sind.

Hinweis auf Nutzungsbedingungen der Drittplattform

Aus Gründen der Nutzerfreundlichkeit sollte die Rundfunkanstalt in ihrer Datenschutzerklärung transparent aufzeigen, dass sie mit eigenen Seiten/Kanälen und Inhalten auf Social Media-Plattformen und anderen Drittplattformen präsent ist.

Dem Nutzer sollte erklärt werden, dass die Datenverarbeitung durch die Betreiber der Drittplattformen außerhalb der Verantwortung der Rundfunkanstalten liegt. In diesem Kontext sollte – zum Beispiel per Link – auch auf die allgemeinen Geschäftsbedingungen beziehungsweise Datenschutzrichtlinien der jeweiligen Drittplattformen verwiesen werden.

Es bietet sich hier an, bei den Drittplattformen genau zu differenzieren und für jeden Drittanbieter jeweils einen eigenen Passus in die Datenschutzerklärung aufzunehmen.

Embedding von fremden Inhalten: Plugins, Videos & Co

Embedding bedeutet das Einbinden fremder Inhalte auf den eigenen Webseiten oder Apps. Eingebettet werden zum Beispiel Fotos, Grafiken, Audio- und Videofiles, Textnachrichten sowie Social Media Plugins zum Teilen, ‚Liken' von Inhalten.

Das Einbinden fremder Inhalte wird dabei häufig über sogenannte iFrames (Inlineframes) realisiert. Einfach gesprochen ist der iFrame auf einer bestimmten Website wie ein kleines Fenster, in dem eine ganz andere Website, die auf einem anderen Server liegt, angezeigt wird. Der Nutzer schaut dann eigentlich gerade mehrere Websites parallel an. Dank Embedding muss der Nutzer also zum Beispiel keinen eigenen Video-Player implementieren oder die Video-Dateien selbst hosten.

Was sagt der Datenschutz?

Beim Embedding externer Inhalte in die rundfunkeigenen Onlineseiten oder Apps können die Anbieter dieser Inhalte (nachfolgend bezeichnet als „Drittanbieter") auf Daten der Nutzer der Webseite der Rundfunkanstalt zugreifen und für sich nutzen.

Sobald der Nutzer eine Seite der Rundfunkanstalt mit eingebetteten Inhalten aufruft, wird – sofern die Rundfunkanstalt keine besonderen Vorkehrungen trifft – regelmäßig die IP-Adresse der Nutzer ohne Vorwarnung, ohne Wissen und möglicherweise gegen seinen Willen an die Drittanbieter übertragen, ohne dass der Nutzer dieses Angebot angeklickt hat. Durch den Einsatz von Cookies erfassen die Drittanbieter von Social Media-Funktionen zudem das individuelle Surfverhalten der Nutzer. Für ein solches User-Tracking ist es noch nicht einmal erforderlich, dass der Nutzer beim jeweiligen sozialen Netzwerk eingeloggt oder dort Mitglied ist. Diese Übertragung von Nutzerdaten an Drittanbieter ist aber nur mit Einwilligung des Nutzers zulässig.

Erfolgt die Datenverarbeitung durch den Drittanbieter auf der Grundlage einer entsprechenden Vereinbarung im Auftrag der Rundfunkanstalt, so wie bei Blog- bzw. Kuratiertools (zum Beispiel Scribble Live) und Tools von Kartenanbietern (zum Beispiel Bing-Maps), wird die Datenverarbeitung durch den Drittanbieter der Rundfunkanstalt zugerechnet. In diesem Fall ist keine Einwilligung des Nutzers erforderlich.

Checkliste

Einbettung aus redaktionellen Gründen erforderlich?

Beim Einbetten von externen Inhalten sollte der redaktionelle Mehrwert der Verwendung der Inhalte gegen die datenschutzrechtlichen Risiken im Einzelfall abgewogen werden. Bei der Abwägung sind die jeweiligen Datenschutzrichtlinien des Drittanbieters zu berücksichtigen.

Gibt es datenschutzfreundliche Voreinstellungen?

Vor dem Embedding von externen Inhalten sollte geprüft werden, ob beim Drittanbieter datenschutzfreundliche Voreinstellungen bestehen.

Einzelne Anbieter wie zum Beispiel YouTube scheinen inzwischen die Möglichkeit zu bieten, Inhalte so einzubetten, dass Cookies nicht zur Profilbildung genutzt werden. Dazu muss ein erweiterter Datenschutzmodus aktiviert werden. YouTube erklärt den erweiterten Datenschutzmodus wie folgt: „*Wenn du diese Option aktivierst, werden von YouTube keine Informationen über die Besucher auf deiner Website gespeichert, es sei denn, sie sehen sich das Video an*“. Zumindest vor dem Klick auf das Video scheint dann kein Tracking stattzufinden. Eine wirkliche Kontrolle, was die Einbettung tatsächlich auslöst, gibt es nicht. Überdies ist auch bei Verwendung des erweiterten Datenschutzmodus die Information des Nutzers über die Datenverarbeitung durch den Drittanbieter nach dem Klick erforderlich.

Einsatz der (modifizierten) Zwei-Klick-Lösung

Für ein datenschutzkonformes Embedding von Plugins und anderen Inhalten von Drittanbietern sollte die von heise.de entwickelte sogenannte „Zwei-Klick-Lösung“ – zumindest in einer modifizierten Version – eingesetzt werden.

Die Zwei-Klick-Lösung ist derzeit weit verbreiteter Standard in den Onlineangeboten der Rundfunkanstalten: Dabei sind die Plugins bei Aufruf der Onlineseite der Rundfunkanstalt inaktiv – es fließen keine Daten an den Drittanbieter. Erst nach der Aktivierung einer Zwischenschaltfläche (Grafik) durch den Nutzer beginnt die Datenübertragung. Der Nutzer wird, sobald er über die Schaltfläche mit dem Mauszeiger fährt, über die Datenweitergabe informiert. Bei Touch-Geräten erfolgt die Information über die Datenweitergabe nach dem ersten Klick.

Allerdings ist dieses Vorgehen nicht sehr nutzerfreundlich und behindert gerade bei Social Plugins die programmlichen Interessen von Fangewinnung und Reichweitensteigerung. Der Nutzer muss für den Besuch einer einzigen Website einschließlich der eingebetteten Inhalte zahlreiche Klicks durchführen und Warnhinweise zur Kenntnis nehmen.

Die Zwei-Klick-Lösung kann auch in einer modifizierten, nutzerfreundlicheren Version eingesetzt werden: Dabei wird der Nutzer pro Session beim Anklicken des ersten eingebetteten Inhalts auf einer Webseite auf einer Zwischenseite über die Datenverarbeitung durch die Drittanbieter aufgeklärt und hat die Wahl, auf weitere entsprechende Hinweise auf der Website zu verzichten. Wenn er darauf verzichtet, wird die Zwischenseite bei nachfolgenden Einbettungen nicht jedes Mal wieder eingesetzt. Er hat damit die Option zur „generellen“ Freischaltung aller Drittanbieter-Inhalte auf der jeweiligen Webseite. Dieses Verfahren muss die Möglichkeit vorsehen, die pauschal erklärte Zustimmung jederzeit zu widerrufen.

Shariff-Button für Social Media-Plugins

Für Social Plugins von Facebook, Twitter und Google+ hat heise.de eine neue, verbesserte Lösung entwickelt, den sogenannte Shariff-Button.

Auch mittels Shariff werden zunächst keine Daten übertragen. Die Nutzer können die jeweilige Website besuchen, ohne dass gleichzeitig ihr Surfverhalten für die sozialen Netzwerke sichtbar wird, denn die Daten des Nutzers werden auf einem Zwischenserver gespeichert, so dass sie von den sozialen Netzwerken nicht direkt „abgefangen“ werden. Der Shariff-Button stellt die Verbindung zum sozialen Netzwerk erst dann her, wenn der Nutzer aktiv wird und auf den Button klickt. Der Vorteil von Shariff ist, dass es nur **einen** Button gibt und dieser farbig gestaltet werden kann, so dass er im Zweifel von den Original-Plugins zu unterscheiden ist.

Man benötigt also nur **einen** Klick für ein „Like“ oder „Share“. Der erste Klick, mit dem die Buttons bisher bei der Zwei-Klick-Lösung aktiviert werden mussten, ist obsolet geworden.

Information über das Embedding von Inhalten und Tools von Drittanbietern in der Datenschutzerklärung

In der Datenschutzerklärung sollte die Rundfunkanstalt umfassend über das Einbinden von externen Inhalten und Social Plugins auf ihren Seiten informieren. Die Hinweise sollten nach Drittanbietern differenziert werden. Dabei sollten auch auf die Zwei-Klick-Lösung sowie die Shariff-Lösung Bezug verwendet und die Funktionsweise erläutert werden.

Über den Einsatz von Blog-/Kuratiertools und sonstigen Tools Dritter, die die Rundfunkanstalt auf der Grundlage einer entsprechenden Vereinbarung auf ihren Seiten einsetzt, sollte im Sinne größtmöglicher Transparenz ebenfalls informiert werden.

Achtung Auftragsdatenverarbeitung

Manche externen Tools – wie zum Beispiel Live-Blogging – sind Werkzeuge, die die Rundfunkanstalt zur Erzeugung ihrer eigenen Inhalte und Integration von Social-Media-Kanälen verwendet. In der Regel fließen aber auch hier Daten zum Drittanbieter. Um die interaktiven Features des Live-Blogs nutzen zu können, werden sowohl die IP-Adresse als auch weitere gerätebezogene Informationen an den Dienstleister übertragen. Zudem werden temporäre Cookies auf der Festplatte des Nutzers gesetzt.

Verarbeitet der Anbieter des Tools in diesem Zusammenhang Nutzerdaten, so tut er dies im Auftrag der Rundfunkanstalt; die Datenverarbeitung wird der Rundfunkanstalt zugerechnet. Es gelten hier die Hinweise

zur Auftragsvergabe an Dritte. Mit der Vereinbarung muss insbesondere sichergestellt werden, dass die Datenverarbeitung durch den Anbieter nur mit Wissen und Wollen der Nutzer erfolgen.

Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Gewinnspiele

Gewinnspiele sind als Teil des redaktionellen Angebots auch in den Telemedienangeboten der Rundfunkanstalten möglich. Es gibt Gewinnspiele im rundfunkeigenen Angebot (zum Beispiel über ein Kontaktformular), die in der Regel auch On-Air beworben werden, mit Mitspielmöglichkeiten auf dem eigenem Angebot und/oder auf Drittplattformen. Es gibt aber auch Gewinnspiele, die ausschließlich auf Drittplattformen durchgeführt werden (zum Beispiel „Liken und teilnehmen“, „Der User-Kommentar mit den meisten Likes gewinnt“).

Was sagt der Datenschutz?

Welche Nutzerdaten wie lange bei einem Online-Gewinnspiel abgefragt und verarbeitet werden können, hängt von der konkreten Ausgestaltung des Spieles ab. Hier gibt es zahlreiche Varianten. Bei allen Varianten ist aber darauf zu achten, dass nur die Nutzerdaten erhoben werden, die für die Durchführung des Gewinnspiels tatsächlich notwendig sind. Die erhobenen Daten dürfen nur zur Durchführung des Gewinnspiels verwendet werden (also nicht zum Beispiel auch zur Zusendung eines Newsletter). Sie dürfen auch nur so lange gespeichert werden, wie es für die Durchführung des Gewinnspiels erforderlich ist. Danach sind die Daten zu löschen.

Checkliste für Gewinnspiele im anstaltseigenen Onlineangebot

Teilnahmebedingungen mit Informationen zum Datenschutz

Jedes Gewinnspiel braucht Teilnahmebedingungen. Diese sind vorab festzulegen. Darin können auch die nötigen Informationen zum Datenschutz integriert werden. Bei einem Gewinnspiel ist (zum Beispiel auf dem Teilnahmeformular) stets ein Checkbox-Feld vorzusehen, in dem der User aktiv anklicken muss, dass die Teilnahmebedingungen gelesen und akzeptiert wurden.

Zweckbindung und Datensparsamkeit

Die Rundfunkanstalt darf nur die Daten als Pflichtfelder abfragen, die für die Durchführung des Gewinnspiels erforderlich sind. Die Daten dürfen auch für keine anderen Zwecke verwendet werden.

Die Pflichtfelder sind entsprechend kenntlich zu machen. Beispiele:

\ Die Abfrage der Mailadresse ist ausreichend, wenn ein Versand des Preises (zum Beispiel Tickets) online erfolgt und um eine Identifikationsmöglichkeit zu haben (zum Beispiel um eine Mehrfachteilnahme zu verhindern).
\ Die (zusätzliche) Telefonnummer ist zulässig, wenn eine telefonische Kontaktaufnahme (Rückruf) notwendig oder ein Telefongespräch on-air geplant ist.
\ Die Abfrage der Postadresse ist zulässig, wenn der Gewinn verschickt werden muss. **Aber**: In der Regel ist hier jedoch eine vorherige Kontaktaufnahme per Mail oder Telefon mit den Gewinnern möglich, so dass eine Adressangabe als Pflichtfeld bei allen Teilnehmern nicht immer erforderlich ist. Viele Nutzer sind außerdem nicht bereit, die Adresse als Pflichtfeld anzugeben.

Alle weiteren Angaben dürfen – sofern redaktionell gewünscht – nur als freiwilliges Datum abgefragt werden, immer verbunden mit dem ausführlichen Datenschutzhinweis, zu welchem Zweck diese konkrete Datenverarbeitung erfolgt und dass die Daten nicht an Dritte weitergegeben werden. Ein Verweis auf die „allgemeinen“ Datenschutzhinweise der Rundfunkanstalt ist insofern nicht ausreichend. Diese zusätzliche Abfrage sollte nur dann durchgeführt werden, wenn ein echter redaktioneller Mehrwert zu erwarten ist.

Der Nutzer ist darüber zu informieren, dass er bei weiteren freiwilligen Angaben seine Einwilligung widerrufen kann.

An die Löschung denken

Die Daten der Teilnehmer am Gewinnspiel sind zu löschen, sobald das Gewinnspiel beendet und eine angemessene „Reklamationszeit“ abgelaufen ist. Die konkreten Löschfristen hängen auch von der „Größe“ des Gewinnspiels ab. Je nach Wertigkeit des Gewinns können die Anforderungen an die Länge der Aufbewahrungsfristen variieren.

Die Daten der Gewinner sind zudem bei anderen Stellen in der Rundfunkanstalt zu Dokumentationszwecken auch nach Ablauf der Gewinnspiels zu speichern (Steuer, Revision und so weiter) und sind dort nach den jeweiligen internen Regelungen zu löschen

Außerdem muss sichergestellt sein, dass nach der Speicherfrist tatsächlich die Löschung der Daten erfolgt. Sofern keine entsprechende Programmierung erfolgen kann, muss notfalls auch eine manuelle Löschung erfolgen. Der Aufwand, der dies möglicherweise verursacht, ist kein Grund, einen „Datenfriedhof“ vorzuhalten.

Minderjährigen-Datenschutz

Beim Umgang mit Daten von Minderjährigen sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet und gespeichert werden. Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting für das Gewinnspiel beauftragt ist, sind die Hinweise zur Auftragsvergabe an Dritte zu beachten.

Beachtung der sonstigen Vorgaben für Gewinnspiele

Es sind die sonstigen Vorgaben der öffentlich-rechtlichen Rundfunkanstalten für Gewinnspiele zu beachten (vergleiche ARD-Richtlinien für Werbung, Sponsoring, Gewinnspiele und Produktionshilfe vom 12. März 2010, http://www.ard.de/download/553234/ARD_Richtlinien_fuer_Werbung__Sponsoring__Gewinnspiele_und_Produktionshilfe_in_der_Fassung_vom_12_3_2010.pdf).

Checkliste für Gewinnspiele ausschließlich auf Drittplattformen:

Verantwortlichkeit des Plattformanbieters

Es gelten grundsätzlich die Teilnahmebedingungen und Datenschutzbestimmungen des jeweiligen Plattformanbieters (siehe hierzu die Hinweise zu Drittplattformen).

Achtung bei Nutzerverarbeitung auch durch die Rundfunkanstalt

Sobald die Nutzerdaten anlässlich des Gewinnspiels aber auch in der Rundfunkanstalt verarbeitet werden, gelten die oben genannten Vorgaben.

Beachtung der sonstigen Vorgaben der Drittplattform

Es sind die sonstigen AGB/Richtlinien der jeweiligen Drittplattform zur Veranstaltung von Gewinnspielen zu beachten (vergleiche zum Beispiel Nutzungsbedingungen von Facebook www.facebook.com/page_guidelines.php).

Instant Messaging

Instant Messaging ist eine sehr verbreitete Kommunikationsmethode, bei der sich mindestens zwei Teilnehmer per Textnachrichten unterhalten. Populäre Instant Messaging-Dienste sind zum Beispiel WhatsApp, Snapchat oder Facebook Messenger.

Dabei löst der Absender die Übermittlung aus (sogenannte „Push-Verfahren“), so dass die Nachrichten möglichst unmittelbar (englisch „instant“) beim Empfänger ankommen. Viele Instant-Messenger unterstützen zusätzlich die Übertragung von Dateien und Audio- und Video-Streams. Benutzer können sich gegenseitig in ihrer Kontaktliste führen und sehen dann an der Präsenzinformation, ob der andere zu einem Gespräch bereit ist.

Was sagt der Datenschutz?

Es gibt viele Anbieter auf dem Markt, die jedoch unterschiedlich mit Datenschutz und IT-Sicherheit umgehen. Viele Messenger-Anbieter informieren den Nutzer nicht oder unzureichend über ihre Datenschutzbestimmungen. Viele Messenger-Apps verzichten zudem auf die Verschlüsselung der Kommunikation. So können Inhalte, Kontakte und andere vertrauliche Daten ausgelesen werden. Im privaten Umfeld liegt die Entscheidung zwar beim Nutzer, ob Datenschutz- und IT-Sicherheitsaspekte eine Rolle spielen. Wenn eine Rundfunkanstalt Instant Messenger Dienste als Kommunikationsmittel nutzt, sollte sie im Rahmen ihrer Möglichkeit auf einen datenschutzkonformen Einsatz achten.

Checkliste

Datensparsamkeit und Zweckbindung

Es gelten die allgemeinen Grundsätze (vergleiche Datenschutz „Basics“): Es sollen so wenig Daten wie möglich erhoben werden; die Daten dürfen jenseits der journalistisch-redaktionellen Nutzung nur so lange gespeichert werden, wie es für diesen Zweck erforderlich und notwendig ist. Sie dürfen nicht anderweitig verwendet werden. Danach sind die Daten zu löschen.

Die Rundfunkanstalt hat Nutzungsstatistiken anonym – also ohne Personenbezug – zu führen.

Information in Datenschutzerklärung

In der allgemeinen Datenschutzerklärung sind die Nutzer über den Einsatz von Instant Messengers durch die Rundfunkanstalt zu informieren.

An die Löschung denken

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Dazu muss man trennen, ob die personenbezogenen Daten – zum Beispiel auch die eingesandten Fotos, „Geschichten" und so weiter – der Nutzer journalistisch-redaktionell genutzt werden (sollen) und eine Archivierung erfolgen soll oder nicht (zum Beispiel bei Gewinnspielen/Kartenverlosungen/Staumeldern und so weiter).

Es ist sinnvoll, sich generell auf ein Löschkonzept für die Daten, der auf Servern der Rundfunkanstalt liegen, zu verständigen. Außerdem muss sichergestellt werden, dass nach der Speicherfrist auch tatsächlich eine Löschung der Daten erfolgt. Sofern hier keine entsprechende Programmierung erfolgen kann, muss notfalls auch eine händische Löschung erfolgen.

Wenn eine vom Löschkonzept abweichende Speicherung der Nutzerdaten gewünscht ist (zum Beispiel bei „Stammschreibern"), ist eine gesonderte Einwilligung der Betroffenen einzuholen.

Eine Löschung ist nicht erforderlich, wenn die Daten anonymisiert werden.

Lokale Datenspeicherung – keine automatische Synchronisation mit Dritten

Bei der Auswahl des Messenger Dienstes sollte darauf geachtet werden, dass nur eine lokale Speicherung der Daten auf dem Gerät erfolgt und keine automatische Synchronisation mit Drittanbietern erfolgt.

Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur **in** der Rundfunkanstalt verarbeitet und gespeichert werden. Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting beauftragt ist, sind die Hinweise zur Auftragsvergabe an Dritte zu beachten.

Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Mailkontakt, Kontaktformular, Newsletter

Das Internet bietet vielfältige Möglichkeiten der Kontaktaufnahme mit dem Nutzer. Neben dem direkten Mail-Kontakt zwischen Nutzer und Rundfunkanstalt können Online-Kontakt-Formulare eingesetzt werden. Über Newsletter können User gezielt über ausgewählte Themen informiert werden.

Was sagt der Datenschutz?

Beim Kontakt mit Usern gilt bei allen Varianten grundsätzlich folgendes: Es sollen immer nur so viele bzw. wenige personenbezogene Daten wie unbedingt nötig abfragt werden. Die abgefragten Daten dürfen immer nur für einen ganz bestimmten Zweck erfolgen. Danach ist eine – notfalls manuelle – Löschung erforderlich.

Checkliste

Zweckbindung und Datensparsamkeit

Die Rundfunkanstalt darf nur solche Daten als Pflichtangaben abfragen, die für den konkreten Zweck – Kontaktaufnahme, Zusendung eines Newsletters und so weiter – unbedingt notwendig sind (kein „nice to have"). Die Pflichtfelder sind entsprechend kenntlich zu machen

Sofern in einem Kontaktformular weitere persönliche Daten abgefragt werden, ist darauf hinzuweisen, dass dies keine Pflichtangaben, sondern freiwillige Angaben sind. Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es erforderlich ist und für keine anderen Zwecke verwendet werden.

Besonderheiten beim Newsletter

Der Nutzer muss den Newsletter ausdrücklich bestellen, das heißt: Newsletter dürfen nie unverlangt zugesandt werden. Neben dem Bestellformular ist auch bereits die Möglichkeit zur Abbestellung des Newsletters bereitzustellen.

\ Zur rechtssicheren Erklärung der Einwilligung ist das „Double-Opt-in"-Verfahren einzusetzen: Der Interessent erhält nach der Anmeldung eine Begrüßungsnachricht, darin wird er aufgefordert einen Link anzuklicken. Erst danach darf seine E-Mail-Adresse für den Empfang des Newsletters aktiviert werden. Damit kann verhindert werden, dass jemand eine fremde Mail-Adresse verwendet. Der gesamte Vorgang ist zu dokumentieren.
\ In jedem Newsletter muss der Nutzer deutlich sichtbar darauf hingewiesen werden, dass er den

Newsletter jederzeit abbestellen kann. Hierzu ist ein Link in die Newsletter-Mail zu setzen.

\ Wie immer gilt die Zweckbindung: Daten eines Nutzer, die der Rundfunkanstalt zum Beispiel im Rahmen der Bestellung eines Newsletters übermittelt wurden, dürfen auch nur für diesen Newsletter und nur solange genutzt werden, wie das Abo läuft. Sobald der Nutzer den Newsletter wieder abbestellt, sind seine Daten zu löschen bzw. zu anonymisieren.

Informationen in der Datenschutzerklärung

In der allgemeinen Datenschutzerklärung sind die Nutzer über die Möglichkeiten der Kontaktaufnahme zu informieren.

An die Löschung denken

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Dazu muss man trennen, ob die personenbezogenen Daten – zum Beispiel auch die eingesandten Fotos, „Geschichten“ und so weiter – der Nutzer journalistisch-redaktionell genutzt werden und eine Archivierung erfolgen soll, oder nicht. Statistiken über Nutzer können anonym geführt werden.

Es ist sinnvoll, sich generell auf ein Löschkonzept zu verständigen. Außerdem muss sichergestellt werden, dass nach der Speicherfrist auch tatsächlich eine Löschung der Daten erfolgt. Sofern keine entsprechende Programmierung erfolgen kann, muss notfalls eine händische Löschung erfolgen.

Wenn eine vom Löschkonzept abweichende Speicherung der Nutzerdaten gewünscht ist (zum Beispiel bei „Stammschreibern“), ist eine gesonderte Einwilligung der Betroffenen einzuholen.

Datensicherheit – verschlüsselte Übertragung

Die Kommunikation mit Nutzern über das Internet ist so sicher wie möglich zu gestalten, sobald persönliche Daten übertragen werden. Insofern sollte stets eine verschlüsselte Übertragung ermöglicht werden, sofern dies technisch realisierbar und vom Aufwand her verhältnismäßig ist.

Bei Kontaktformularen im eigenen Angebot sollte eine Verschlüsselung über ein anerkanntes, dem Stand der Technik entsprechendes Verschlüsselungsverfahren zur sicheren Übertragung von Informationen angeboten werden.

Auch bei Mail-Kontakt ist – sofern machbar – eine End-to-End-Verschlüsselung zu empfehlen. Auch wenn dieses Verfahren aufwändig ist, sollte eine End-to-End-Verschlüsselung jedenfalls dann eingesetzt werden, wenn ein Kontakt im Zusammenhang mit journalistischer Recherche be- bzw. entsteht.

Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet werden. Sofern ein Dienstleister für den konkreten Kontakt mit dem Nutzer mit der Durchführung und/oder dem Hosting beauftragt ist, sind die Hinweise zur Auftragsvergabe an Dritte zu beachten.

Minderjährigen-Datenschutz

Die Rundfunkanstalten wenden sich mit ihren Telemedienangeboten auch an Kinder und Jugendliche. Beispiele für Angebote, bei denen personenbezogene Daten von Minderjährigen erhoben werden, sind Newsletter, Gästebücher und Chats, Gewinnspiele und Mitmachaktionen, die eine aktive Eingabe von Daten erfordern. Beim Umgang mit personenbezogenen Daten von Minderjährigen gelten besondere Anforderungen.

Was sagt der Datenschutz?

Die Nutzung von Angeboten durch Kinder und Jugendliche ist unproblematisch, wenn keine personenbezogenen Daten des Kindes bzw. Jugendlichen explizit abgefragt werden. Die beim Besuch einer Seite ohnehin anfallende IP-Adresse ist notwendig zur Bereitstellung des Dienstes und wäre insoweit unkritisch.

Komplizierter wird es, wenn persönliche Daten der jungen Nutzer wie zum Beispiel Name oder E-Mail-Adresse abgefragt werden. Dies ist grundsätzlich nur mit Einwilligung des Kindes bzw. des Jugendlichen zulässig. Kinder und Jugendliche können in die Verarbeitung ihrer Daten allerdings nur wirksam einwilligen, sofern sie verstehen, welche Konsequenzen dies für sie haben kann, wenn ihre Daten von einem Internet-Unternehmen abgefragt und verwendet werden (Einsichtsfähigkeit). Dies hängt direkt mit dem Grad der Entwicklung und damit auch mit dem Alter zusammen. Daher geht das Einwilligungsrecht graduell von den Eltern auf die Kinder über.

Checkliste

Vorab: Für welche Altersgruppe ist das Angebot gedacht?

Es ist vorab zu klären, welche Altersgruppe mit dem Angebot angesprochen werden soll.

Keine Besonderheiten für Jugendliche, die das 16. Lebensjahr vollendet haben

Jugendliche **ab 16 Jahren** können in dieser Hinsicht wie Erwachsene behandelt werden. Für sie gelten keine Besonderheiten. Sie können ohne Mitwirkung der Eltern in eine Datenverarbeitung einwilligen; ebenso können sie ihre Einwilligung auch jederzeit selbst widerrufen. Im Übrigen gelten sämtliche datenschutzrechtlichen Vorgaben und Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung und so weiter – vergleiche Datenschutz Basics).

Einzelabwägung bei Jugendlichen von 13 bis 16 Jahren

Bei **13- bis 16-Jährigen** hängt die Möglichkeit einer eigenen wirksamen Einwilligung vom Grad der Reife und dem Zweck der Einwilligung und der damit einhergehenden Tragweite der Entscheidung in die Datenpreisgabe ab. Maßgeblich ist die individuelle Einsichtsfähigkeit. Insofern kommt es in dieser Altersgruppe immer auf den Einzelfall an.

Es ist dabei zu berücksichtigen, dass der durchschnittliche Jugendliche in dieser Altersgruppe mit Computer, Internet und Social Media aufgewachsen ist und regelmäßig schon Erfahrungen im Umgang mit dem Internet gesammelt hat. Ab Vollendung des 13. Lebensjahrs kann in der Regel von einer Einsichtsfähigkeit ausgegangen werden, wenn transparent und altersgerecht über die Art und den Zweck der Datenverarbeitung aufgeklärt wird.

Entscheidend ist auch der Zweck der Datenabfrage. Danach sollte es für Kinder und Jugendliche beispielsweise möglich sein, einen Newsletter der Lieblingswebseite zu abonnieren oder sich auf einer Lernplattform zu registrieren.

Es wird empfohlen, zum Beispiel einen spielerischen Zugang zu wählen und damit die Einsichtsfähigkeit „abzuprüfen“. Die Teilnahme bei einem Datenschutzspiel und den damit verbundenen Lösungen von Aufgaben kann die Voraussetzung für die Nutzung eines Angebotes sein.

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit und so weiter – vergleiche Datenschutz Basics).

Achtung bei Kinder unter 13 Jahren: Einwilligung der Eltern erforderlich

Bei Kindern **unter 13 Jahren** muss eine Einwilligung der Eltern eingeholt werden. Dies gestaltet sich in der Praxis nicht immer leicht. Am sichersten ist der schriftlich-postalische Weg, auch wenn dieser dem Medium Internet nicht gerecht wird und sehr aufwändig ist. Möglich sind auch digitale Einwilligungsformen, beispielsweise die Zusendung eines digitalen Fotos der unterschriebenen Einwilligungserklärung. Häufig werden für die Einwilligung Klick-Boxen eingesetzt. Hier müssen Kinder die E-Mail-Adresse der Eltern angeben und diese müssen dann der Datenverwendung zustimmen (sogenannte „Eltern-Okay“). Jedoch können Kinder natürlich auch ihre E-Mail-Adresse hier angeben und demnach selbst zustimmen. Dieses Verfahren ist also nicht vollständig sicher, weil es durch den Minderjährigen umgangen werden kann. Wenn die Einwilligung der Eltern erforderlich ist, muss diese auch nachgewiesen werden.

Im Hinblick auf die praktischen Schwierigkeiten bei der Einwilligung der Eltern ist immer auch zu prüfen, ob Mitmachaktionen und Ähnliches auch gänzlich ohne personenbezogene Daten realisiert werden können.

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit und so weiter – vergleiche Datenschutz Basics).

Absolutes Muss: Kinderfreundliche Datenschutzerklärung

Wenn Minderjährige einsichtsfähig sind und damit selbst einwilligen können, ist es von entscheidender Bedeutung, dass ihnen auch die erforderlichen Informationen gegeben werden. Die Datenschutzerklärung muss leicht auffindbar und in einfacher Sprache verständlich gefasst sein. Die einzelnen Einwilligungen in die Datenverarbeitung müssen ebenfalls so gestaltet sein, dass der Minderjährige erkennt, worin er tatsächlich einwilligt.

Gleiches gilt für Angebote an Kinder bis 13 Jahre: Bei der Erhebung von Daten bei Kinderangeboten spielt die Transparenz eine große Rolle. Je klarer dem Kind und auch den Erziehungsberechtigten die Notwendigkeit der Daten für das Produkt verdeutlicht wird, umso größer wird die Akzeptanz für die Erhebung. Ebenso sollte in den Datenschutzhinweisen erklärt werden, wie lange die Daten für den Zweck vorgehalten werden, dass sie

abschließend gelöscht werden, und so weiter Es gelten insoweit die Hinweise zur Datenschutzerklärung.

Keine Einwilligung bei Präventions- und Beratungsdiensten direkt für Kinder und Jugendliche

Im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind oder Jugendlichen angeboten werden, ist die Einwilligung der Eltern generell nicht erforderlich (Besonderheit des neuen EU-Rechts). Das Konzept des Angebotes sollte daher auf seine medienpädagogische Relevanz geprüft werden. Dient es auch der Prävention oder Beratung der Kinder/Jugendlichen?

Abstimmung mit dem Datenschutzbeauftragten

Wegen der Besonderheiten des Minderjährigen-Datenschutzes wird empfohlen, sich bei allen Konzepten, Projekten und Angeboten immer mit dem jeweiligen Datenschutzbeauftragten zu beraten und abzustimmen.

Förderung der Medienkompetenz und Einsichtsfähigkeiten der Kinder und Jugendlichen

Bei allen Angeboten für Minderjährige sollten die Rundfunkanstalten einen Beitrag zur Bildung von Medienkompetenz bei Kindern und Jugendlichen leisten. Gerade bei dieser Altersgruppe gibt es vielfache Möglichkeiten, die Einsichtsfähigkeit durch Spiele und Ähnliches zu „trainieren“.

Personalisierung

Über die Personalisierung einer Webseite kann dem Nutzer ein jeweils auf seine Vorlieben und Interessen individuell zugeschnittenes Angebot zur Verfügung gestellt werden.

Derzeit etablieren sich am Markt Funktionalitäten, die dem Nutzer zielgerichtete, auf seine Präferenzen abgestimmte Angebote machen können (Merklisten, Playlists, Empfehlungen, Push-Nachrichten, Social-Media-Einbindung etc.).

Hierfür werden alle dafür nützlichen Daten ausgewertet und die jeweilige Website wird entsprechend angepasst und angezeigt, zum Beispiel mit Hilfe von Cookies und persönlichen Daten, die bei einer Registrierung aufgenommen wurden. Diese Personalisierungsfunktionen können teilweise nur angeboten werden, wenn der Nutzer sich bei einem Dienst anmeldet beziehungsweise seine Daten in einem gewissen Umfang zur Verfügung stellt.

Was sagt der Datenschutz?

Für eine Personalisierung müssen in der Regel Informationen über das Verhalten des Nutzers gesammelt werden, um ihm Vorschläge zum Angebot zu unterbreiten oder ihm die Möglichkeit zu bieten, sich sein eigenes Angebot zusammenzustellen. Diese Informationen können Personenbezug auf weisen oder nicht. Für die Anwendung des Datenschutzrechts kommt es also darauf an, welche und wie viele Daten jeweils tatsächlich genutzt werden.

Generell sollte bei der Personalisierung mit Fingerspitzengefühl und Sorgfalt vorgegangen werden.

Checkliste

Personalisierung durch persönliches Nutzerkonto

Personalisierung kann dadurch erreicht werden, dass der Nutzer sich freiwillig für ein eigenes Konto mit persönlichen Daten, Vorlieben und Interessen registriert. Der Nutzer muss sich hier über ein eigenes Login anmelden und kann sein Konto einsehen und selbst verwalten. Auf diese Weise bekommt er nur für ihn zugeschnittene Inhalte angeboten, die er auf sämtlichen Endgeräten nutzen kann. In diesem Fall gelten die bekannten Datenschutzprinzipien (siehe Datenschutz Basics):

Einwilligung

Der Nutzer muss explizit in die Erhebung und Verwendung seiner Daten einwilligen. Dafür braucht es eine transparente Aufklärung sowie eine Dokumentation der Einwilligungserklärung. Es ist darauf zu achten, dass diese Einwilligungserklärung stets abgerufen und auch widerrufen werden kann.

Datensparsamkeit, Zweckbindung, Löschung, Datensicherheit

Für personalisierte Funktionalitäten sollen nur die Daten der Nutzer erhoben werden, wie sie für die spezifischen Angebote notwendig, redaktionell intendiert und vom Nutzer gewollt sind. Das Sammeln von Daten auf Vorrat ist unzulässig. Pflichtfelder und Felder für freiwillige Angaben des Nutzers müssen daher klar gekennzeichnet sein.

Die Daten dürfen nur zu dem vorher klar festgelegten Zweck verwendet werden und dürfen nicht zu anderen Zwecken genutzt oder an Dritte weitergegeben werden. Sie müssen nach Abmeldung oder bei Widerruf der Einwilligung wieder gelöscht werden.

Das Angebot sollte immer die Option bieten, sich von Nutzungsmessungen und Personalisierungsfunktionen abzumelden.

Sehr wichtig ist die sichere Datenhaltung: Vertraulichkeit, Integrität und Verfügbarkeit der Accounts und Nutzerdaten müssen durch entsprechende Vorkehrungen sichergestellt sein.

Personalisierung über Pseudonymisierung/Anonymisierung

Werden personenbezogene/-beziehbare Daten eines Nutzers pseudonymisiert oder anonymisiert, kann die Identität des Nutzers nicht mehr nachvollzogen werden. Es werden lediglich Unterscheidungsmerkmale gespeichert, so dass auf diese Weise ein individualisiertes Angebot ermöglicht wird. Der einzelne Nutzer ist nicht mehr identifizierbar.

In diesem Fall ist auf folgendes zu achten:

Wirksame Pseudonymisierung/Anonymisierung

Es ist zum Beispiel möglich, über eine Geräte-ID oder die IP-Adresse Daten über das Verhalten zu sammeln, um individuelle Empfehlungen auszusprechen. Aber Vorsicht: IP-Adresse und Gerätekennung gelten als personenbezogene Daten. Daher sollten Optionen genutzt werden, die IP-Adresse zu pseudonymisieren oder für die Gerätekennung eine zufallsgenerierte eindeutige Nummer (Token) zu erzeugen, der im Rahmen der Nutzung eindeutig ist, aber außerhalb der App keinen Bezug zum Gerät mehr aufweist.

Möglichkeit des Widerspruchs bei Bildung pseudonymer Nutzerprofile

Sofern zum Zweck der Personalisierung pseudonyme Nutzerprofile gebildet werden, muss der Nutzer die Möglichkeit bekommen, der Bildung von Nutzerprofilen zu widersprechen (siehe hierzu die Hinweise zur Web-Analyse).

Immer: Umfassende Informationen in der Datenschutzerklärung

Für alle Formen der Personalisierung gilt: Die Rundfunkanstalt muss in der Datenschutzerklärung ihres Angebots umfassend und verständlich über Art und Verwendungszweck der Daten aufklären. Auch die Verwaltung der Nutzerdaten sollte erklärt werden.

Minderjährigen-Datenschutz

Sofern sichergestellt ist, dass keine personenbezogenen Daten erhoben werden und der Minderjährige nicht identifiziert werden kann, ist grundsätzlich für Minderjährige ein individuell zugeschnittenes Angebot denkbar. Es sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Social Login

Social Login wird auch als Social Sign-In bezeichnet. Viele soziale Netzwerke wie Facebook, Twitter und Google+ bieten Betreibern von Webseiten oder Apps für einen Registrierungs-Prozess einen geschützten Bereich, damit sich die Nutzer (alternativ) mit ihrem Facebook-, Google- oder Twitter-Account anmelden können. Den Nutzern erspart dies zusätzliche Passwörter und Logins.

Was sagt der Datenschutz?

Klickt der Nutzer auf den Social-Login-Button und meldet sich zum Beispiel über seinen Facebook-Account an, erfolgt die Verknüpfung von Facebook und der Webseite, worüber Facebook stets das öffentliche Profil (insbesondere Name, Profil, Geschlecht) und die Freundesliste übermittelt, da diese Informationen als „öffentlich“ eingestuft sind. Dazu können noch weitere Daten übermittelt werden, die vom Nutzer im Rahmen seiner Privatsphäre-Einstellungen nicht explizit eingeschränkt wurden. Im Gegenzug erhält Facebook Informationen zur Nutzung der Seite durch den Nutzer. Diese Daten können dem Facebook-Benutzerprofil beigefügt und von Facebook weiterverarbeitet werden (zum Beispiel Auswertung der Daten zu Werbezwecken).

Die Funktionalität des Social Logins wurde durch die Betreiber der sozialen Netzwerke entwickelt; diese sind daher für die datenschutzkonforme Datenübermittlung **an** den jeweiligen Webseitenbetreiber verantwortlich.

Aber: Auch die Rundfunkanstalt, die Social Login in ihren Apps und Webseiten anbietet, bleibt datenschutzrechtlich verantwortlich für den Bezug und die Weitergabe von Daten der Nutzer auf/von ihren Angeboten an Facebook oder Anderen.

Beim Einsatz von Social Logins hängt die Zulässigkeit dieser Datenverarbeitungen regelmäßig von einer wirksamen Einwilligungserklärung des Nutzers ab. Diese muss **vor** der Inanspruchnahme des Social Login eingeholt werden.

Angesichts der intransparenten Datennutzung der sozialen Netzwerke, namentlich Facebook, besteht das Risiko, dass das Social Login insgesamt rechtlich unzulässig ist. Auch wenn Facebook seine Nutzer über den Datentransfer aufklärt, genügt dies möglicherweise nicht den gesetzlichen Vorgaben in Deutschland an eine aufgeklärte und transparente Einwilligung.

Checkliste

Information und Einwilligung unmittelbar beim Social Login

Vor Abschluss des Registrierungsvorgangs via Social Login ist der Nutzer über eine eigene zustimmungspflichtige Datenschutzerklärung zu informieren, welche Daten konkret in der Folge von dem sozialen Netzwerk und an dieses und zu welchen Zwecken übermittelt werden. Es empfiehlt sich eine Einbindung der Hinweise im Log-in-Dialog beziehungsweise in unmittelbarer Nähe des Social Login Buttons. Möglich ist dabei eine Verlinkung, so dass der Nutzer per Klick zur unternehmenseigenen Datenschutzerklärung gelangt, in der er über den Log-in-Prozess aufgeklärt wird.

Hinweis zum Social Login in eigener Datenschutzerklärung

Neben der Einholung einer Einwilligung muss die Datenschutzerklärung über das Social Login-Verfahren und die ablaufenden Datenprozesse aufklären.

Hier genügt **nicht** der Hinweis darauf, dass die Social Login-Funktion den Bestimmungen und der Verantwortung des sozialen Netzwerkes unterliegt. Insbesondere sollte erläutert werden, welche Daten vom sozialen Netzwerk bezogen und zu welchen Zwecken diese Daten verwendet werden.

Sofern die Rundfunkanstalten Daten an das soziale Netzwerk senden, sind diese aufzulisten und darüber zu informieren, zu welchen Zwecken das Netzwerk diese Daten nutzt. Schließlich sollte erklärt werden, wie die Verknüpfung zwischen der Webseite der Rundfunkanstalt und dem sozialen Netzwerk wieder gelöst werden kann.

Alternative Registrierungsmöglichkeit

Dem Nutzer sollte es immer freigestellt werden, zwischen dem Social Login und einer separaten Registrierungsmöglichkeit frei zu wählen.

Standortdaten

Standortdaten (Geodaten) sind Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts angeben, mit dem ein Telekommunikationsdienst genutzt wird. Insbesondere Smartphones und Tablets können durch verschiedene Techniken – GPS, WLAN, das Mobilfunknetz oder via IP-Adresse – die Position des Nutzers ermitteln.

Das machen sich viele Apps zu Eigen und bieten Lokalisierungsdienste an. Wenn Dienste Geodaten berücksichtigen, ist das häufig hilfreich, indem sie passgenaue Informationen liefern. Mit Hilfe dieser Daten können den Nutzern ausgewählte Meldungen und Informationen übermittelt werden, die sich auf ihre nähere Umgebung beziehen, zum Beispiel Angaben zum ortsbezogenen Geschehen, Wetter, Verkehr oder zu kulturellen Ereignissen in der Region. Auf der anderen Seite geben Standortdaten Aufschluss über die „Bewegungen“, Gewohnheiten und Interessen der Nutzer.

Was sagt der Datenschutz?

Bei der Ermittlung von ortsbezogenen Daten wird streng genommen nie der jeweilige Nutzer selbst, sondern immer das zugehörige Gerät mit mehr oder weniger großer Genauigkeit geographisch bestimmt. Gleichwohl besteht das Risiko, dass die Standortdaten bestimmbaren Personen zugeordnet werden können, wenn sie zum Beispiel mit der jeweiligen IP-Adresse der Nutzer übermittelt beziehungsweise gespeichert werden.

Durch die Sammlung und Verknüpfung von unterschiedlichen Standortdaten ist es möglich, Bewegungsprofile zu erstellen. Dadurch kann festgestellt werden, wann und wie lange eine Person an einem bestimmten Standort war. Auch Ortungsdaten in anonymisierter Form lassen sich zum Beispiel mit weiteren Datenbeständen kombinieren und so wieder einzelnen Nutzern zuordnen. Einige Dienste sammeln Standortdaten über das notwendige Maß hinaus im Hintergrund und ohne Wissen und Wollen des Nutzers. Regelmäßig werden die Daten zur weiteren kommerziellen Nutzung auch an Dritte weitergegeben.

Die Erhebung und Verwendung von solchen personenbeziehbaren Daten ist nur dann zulässig, soweit die Daten erforderlich sind, um die Inanspruchnahme des Dienstes zu ermöglichen oder wenn die Nutzer dem im Vorwege zugestimmt haben.

Checkliste

Wenn eine Rundfunkanstalt Standortdaten erheben will (zum Beispiel für einen Lokalisierungsdienst in einer App), ist auf Folgendes zu achten:

Information und Einwilligung vor bzw. bei Beginn der Nutzung / Deaktivierung

Die Erhebung und Verwendung von Standortdaten durch die Rundfunkanstalt muss stets **vorab** von den Nutzern nach einer entsprechenden Information freigegeben werden.

Darum ist eine etwaige Lokalisierungsfunktion eines Angebots – zum Beispiel eine App einer Rundfunkanstalt – in den Voreinstellungen standardmäßig zu deaktivieren. Daneben muss es den Nutzern nach Aktivierung möglich sein, die gewählte Funktion jederzeit wieder abzuschalten. Aktivierung und Deaktivierung sollten möglichst durch nur einen Klick erfolgen können.

Informationen zur Erhebung der Standortdaten und zur Aktivierung / Deaktivierung

Die Nutzer sind vorab genau über Art, Umfang und Zweck der Erhebung und Verwendung der Standortdaten zu informieren. Das kann beispielsweise innerhalb der Datenschutzerklärung erfolgen, der vor Beginn der Nutzung des Dienstes zuzustimmen ist. Außerdem muss die Möglichkeit der jederzeitigen Aktivierung bzw. Deaktivierung dieser Datenerhebung aufgezeigt und erklärt werden.

Datensparsamkeit: Erhebung und Nutzung nur der notwendigen Daten

Mit Beginn der Nutzung der Dienste muss sichergestellt sein, dass die Daten nach dem Grundsatz der Datensparsamkeit lediglich erhoben werden, soweit sie zur Nutzung des Dienstes notwendig sind.

Standortdaten können auch permanent und in regelmäßigem Turnus – zum Beispiel alle dreißig Minuten – erhoben werden, um Nutzern einen bestimmten Dienst bieten zu können (zum Beispiel Stau- und Blitzermeldungen als Push-Nachricht). Der Nutzer ist hierüber zu informieren beziehungsweise hat hierzu seine Einwilligung zu geben.

Eine dauerhafte Speicherung von Standortdaten auf dem Endgerät darf nur dann stattfinden, wenn dies für die Funktionalität des Dienstes notwendig ist. Gleiches gilt in Bezug auf die Informationen, die an die Anbieter der Dienste gesendet werden. Andernfalls würde auch hier die Gefahr der Erstellung von Bewegungsprofilen bestehen.

Sofern möglich: „Verwaschung“ des Standorts

Häufig ist es nicht notwendig, dass der Standort des Nutzers metergenau erhoben und verwendet wird. Darum empfiehlt sich eine gezielte „Verwaschung“ des Standortes. Dies kann zum Beispiel durch eine Nullung von Dezimalstellen in den GPS-Koordinaten vor Versand der Daten an den jeweiligen Dienste-Anbieter erreicht werden.

Wichtige Hinweise für die Löschung der Dienste

Wenn die Daten lokal gespeichert werden, ist dafür Sorge zu tragen, dass nach der Löschung des (Lokalisierungs-)Dienstes auch die lokal gespeicherten personenbezogenen Daten des Nutzers gelöscht werden.

Sollte es sich dabei um Daten handeln, die zum Beispiel auch anderen Apps auf dem Endgerät zur Nutzung zur Verfügung gestellt werden, sollte der Nutzer bei der Deinstallation gezielt gefragt werden, ob er diese persönlichen Daten löschen oder auf dem Gerät belassen möchte.

Votings

Votings (Nutzerabstimmungen) sind für viele Redaktionen ein attraktives Element der Programmgestaltung. Durch den direkten Rückkanal sollen die Nutzer am Programm und der Gestaltung des Onlineangebots teilhaben.

Bei der konkreten Ausgestaltung gibt es zahlreiche Varianten („Welche Filme sollen in der Märchenreihe gezeigt werden?“, „Schönste Brücke von XY?“). Dies gilt auch für die technische Umsetzung. Es gibt Votings im eigenen Angebot der Rundfunkanstalt, die in der Regel auch On-Air beworben werden, einschließlich Mitmach-Möglichkeiten im eigenen Angebot und/oder Drittplattformen. Es gibt aber auch Votings, die ausschließlich auf Drittplattformen durchgeführt werden (zum Beispiel „Liken und teilnehmen“).

Was sagt der Datenschutz?

Welche Nutzerdaten wie lange bei einem Voting verarbeitet werden, hängt von der konkreten Ausgestaltung des Votings ab. Daher ist es wichtig, vorab Ablauf und Bedingungen für das Voting festzulegen und die Nutzer hierüber ausreichend zu informieren. Es sind so wenige Nutzerdaten wie möglich zu erheben.

Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es für die Durchführung des Votings erforderlich ist. Sie dürfen auch nicht anderweitig verwendet werden. Danach ist eine Löschung erforderlich.

Checkliste für Votings im anstaltseigenen Angebot

Zweckbindung und Datensparsamkeit

Es sind so wenig Nutzerdaten wie möglich zu erheben: Zulässig sind nur die Daten, die für die Durchführung des Votings unbedingt notwendig sind (kein „nice to

have“). Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es für die Durchführung des Votings erforderlich ist. Sie dürfen für keine anderen Zwecke verwendet werden.

Informationen in der Datenschutzerklärung

Vorab sind Ablauf und Bedingungen für das Voting festzulegen und hierüber in den Datenschutzhinweisen zu informieren.

Absicherung gegen Manipulation

Bei internetbasierten Abstimmungsformen kann – unter Berücksichtigung der Nutzerfreundlichkeit – eine technische Absicherung gegen Manipulation von außen eingesetzt werden (zum Beispiel durch Sperrung der IP-Adresse für ein bestimmtes Zeitfenster, Captcha, Identifizierung per Mail, Cookies). In diesem Fall sind nur solche Daten der Nutzer mitzuloggen, die für die korrekte Durchführung des Votings erforderlich sind. Zudem ist ein konkreter Hinweis in der Datenschutzerklärung erforderlich.

An die Löschung denken

Es sind Löschfristen festzulegen und darauf zu achten, dass die Daten gelöscht werden, sobald das Voting beendet und eine angemessene „Reklamationszeit“ einkalkuliert wurde. Die Daten sind notfalls manuell zu löschen.

Achtung bei externen Dienstleistern

Die Nutzerdaten sollten möglichst nur in der Rundfunkanstalt verarbeitet und gespeichert werden. Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting eines Votings beauftragt ist, sind die Hinweise zur Auftragsvergabe an Dritte zu beachten.

Verknüpfung mit Gewinnspiel

Eine Teilnahme am Voting kann mit einem Gewinnspiel kombiniert werden (zum Beispiel „Unter den ‚Votern‘ werden Tickets verlost.“). In diesem Fall sind zusätzlich die Hinweise zu Gewinnspielen zu beachten.

Verschlüsselung

Die Kommunikation mit Nutzern über das Internet ist so sicher wie möglich zu gestalten, sobald persönliche Daten übertragen werden – dies gilt auch bei Votings. Insofern sollte stets eine verschlüsselte Übertragung ermöglicht werden, sofern dies technisch realisierbar und vom Aufwand her verhältnismäßig ist.

Minderjährigen-Datenschutz

Für den Umgang mit Daten von Minderjährigen sind die Hinweise zum Minderjährigen-Datenschutz zu beachten.

Checkliste für Votings ausschließlich auf Drittplattformen

Verantwortlichkeit des Plattformanbieters

Es gelten grundsätzlich die Datenschutzbestimmungen des jeweiligen Plattformanbieters (siehe hierzu auch die Hinweis unter Drittplattformen).

Achtung bei Nutzerverarbeitung auch durch die Rundfunkanstalt

Sobald die Nutzerdaten anlässlich des Votings **auch** in der Rundfunkanstalt verarbeitet werden, gelten die oben genannten Vorgaben.

Beachtung der sonstigen Vorgaben der Drittplattform

Es sind die sonstigen AGB/Richtlinien zur Veranstaltung von Votings durch Unternehmen zu beachten (vergleiche zum Beispiel die Regelung zu „Promotionen“ in den Nutzungsbedingungen von Facebook www.facebook.com/page_guidelines.php).

Web-Analyse

Web-Analyse (genannt auch Traffic-Analyse, Webtracking oder Webcontrolling) ist die Sammlung von Daten und deren Auswertung bezüglich des Verhaltens von Besuchern auf Webseiten. Ein Webanalyse-Tool untersucht, woher die Besucher kommen, welche Bereiche auf einer Seite aufgesucht werden und wie oft und wie lange welche Unterseiten und Kategorien angesehen werden.

Es gibt verschiedene Analyse-Verfahren (zum Beispiel Piwik, INFOnline, Comscore). Gewöhnlich werden entweder die Logdateien der Webserver ausgewertet oder bestimmte Zählpixel oder Tags in Webseiten zur Datengewinnung genutzt. Cookies sind dabei unabdingbar, um einen Seitenaufruf einer Sitzung und eine Sitzung einem Besucher zuordnen zu können.

Was sagt der Datenschutz?

Bei Web-Analyseverfahren können personenbezogene Daten anfallen, so zum Beispiel auch die IP-Adresse des Nutzers. Hierfür ist grundsätzlich die Einwilligung des Nutzers erforderlich.

Zu Zwecken der Marktforschung und zur bedarfsgerechten Gestaltung von Webseiten dürfen jedoch auch ohne Einwilligung Nutzungsprofile erstellt werden, sofern diese pseudonymisiert sind und der Nutzer dem nicht widerspricht.

Checkliste

Personenbezogene Nutzungsprofile nur mit Einwilligung

Die Erstellung personenbezogener Nutzungsprofile ist grundsätzlich nur mit bewusster, eindeutiger Einwilligung des Nutzers zulässig.

Vorsicht bei IP-Adressen

Die vollständige IP-Adresse ist ein personenbezogenes Datum. Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist daher nur mit Einwilligung des Nutzers zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Pseudonyme Nutzerprofile ohne Einwilligung zulässig

Die Erstellung von Nutzungsprofilen zur Werbung und zur Marktforschung ist gesetzlich erlaubt, sofern **drei Voraussetzungen** beachtet werden:

Pseudonyme:

Es müssen Pseudonyme verwendet werden. Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym – zumeist eine mehrstellige Buchstaben – oder Zahlenkombination (Code) – ersetzt, um die Identifizierung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Widerspruchsrecht:

Dem Nutzer ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Zudem muss der Nutzer in der Datenschutzerklärung auf sein Widerspruchsrecht gegen die Erstellung von Nutzungsprofilen hingewiesen werden.

Strikte Datentrennung:

Das Nutzungsprofil darf nicht mit dem Träger des Pseudonyms zusammengeführt werden. Diese Daten müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.

Anonyme Nutzungsprofile unterliegen nicht dem Datenschutz

Anonyme Auswertungen unterliegen – mangels Personenbezug – keiner datenschutzrechtlichen Beschränkung. Bei der Erstellung anonymer Nutzungsprofile muss allerdings die Anonymität bereits bei der Erhebung der Information, beispielsweise des Klick-Verhaltens, gegeben sein.

Pflicht zur Information in der Datenschutzerklärung

Die Rundfunkanstalt muss im Rahmen der Datenschutzerklärung auf ihrer Internetseite in deutlicher Form auf die Erstellung von Nutzungsprofilen und den Zweck und Umfang der Datenspeicherung hinweisen.

Zudem muss der Nutzer hier auf das Widerspruchsrecht hingewiesen und eine Möglichkeit geschaffen werden, dieses Widerspruchsrecht unmittelbar auszuüben. Es bietet sich an, einen Link vorzusehen, bei dem eine direkte Opt-out-Funktion hinterlegt ist.

Achtung beim Einsatz von Cookies

Regelmäßig werden bei Tracking-Technologien auch (permanente) Cookies eingesetzt. Hierauf muss in der Datenschutzerklärung hingewiesen werden. Zudem sollte darüber informiert werden, wie Cookies bei den gängigen Browsern deaktiviert werden können. Es gelten im Einzelnen die Hinweise zu Cookies.

Achtung: Auftragsdatenverarbeitung!

Die Web-Analyse wird meistens durch Drittanbieter vorgenommen. Daher ist es unbedingt notwendig, die Vorgaben zur Auftragsdatenverarbeitung einzuhalten, sofern die vollständigen IP-Adressen und sonstige Nutzerdaten bei dem Dritten erhoben und verarbeitet werden. Es sind die Hinweise zur Auftragsvergabe an Dritte zu beachten.

IMPRESSUM

Herausgeber

Westdeutscher Rundfunk Köln
Anstalt des öffentlichen Rechts
Marketing
Appellhofplatz 1
50667 Köln

Redaktion

Datenschutzbeauftragte Karin Wagner
Datenschutzreferat

Mai 2017

WESTDEUTSCHER
RUNDFUNK

Appellhofplatz 1
50667 Köln

wdr.de