LEITLINIEN ZUM DATENSCHUTZ

IN DEN TELEMEDIEN-ANGEBOTEN VON ARD, ZDF UND DEUTSCHLANDRADIO

ARD 1 | ZDF | Deutschlandradio

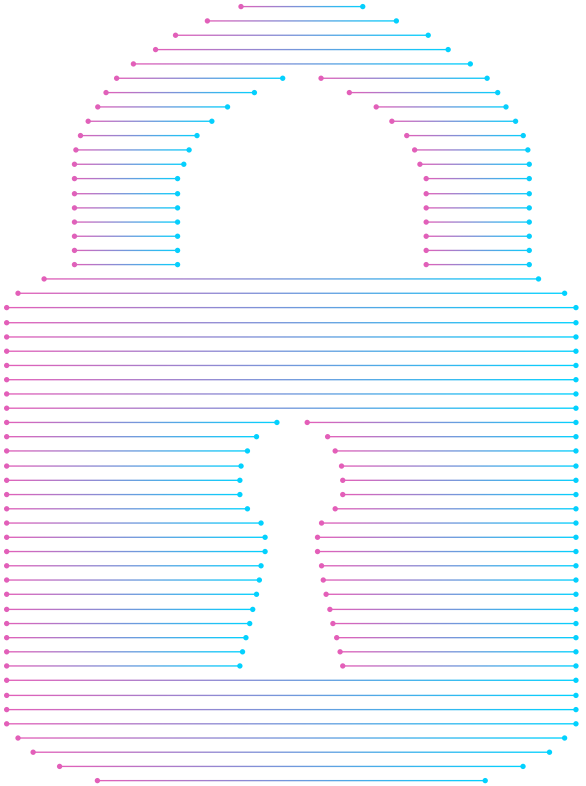
VORBEMERKUNG

THEMEN

→ **Was will der Datenschutz?**
→ Was will der Leitfaden?

WAS WILL DER 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 (sog. 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 in allen Lebens- und Gesellschaftsbereichen stellen den Datenschutz dabei mit rasanter Geschwindigkeit vor immer wieder neue Herausforderungen.



THEMEN

→ Was will der Datenschutz?
→ **Was will der Leitfaden?**

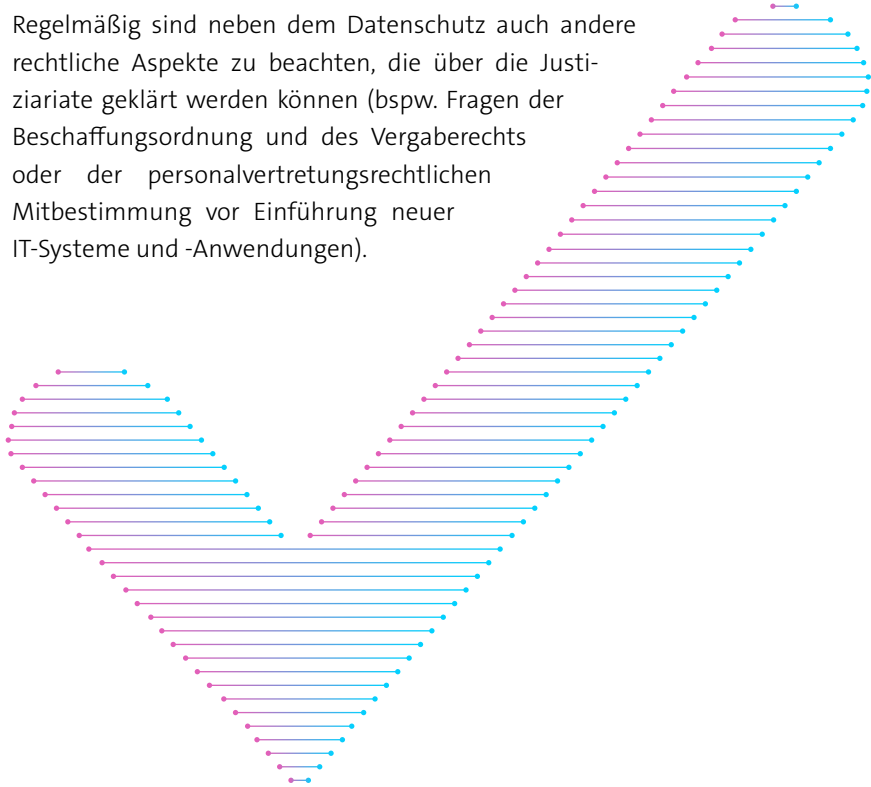
WAS WILL DER LEITFADEN?

Dieser Leitfaden ist ein vom Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio (AK DSB) erarbeiteter Ratgeber, der sich an die Mitarbeiter:innen der Rundfunkanstalten wendet, die Telemedien- und Social-Media-Angebote konzeptionell entwickeln, technisch realisieren und redaktionell einsetzen. Er konkretisiert die verbindlichen Vorgaben der Datenschutzgesetze sowie einschlägiger Rechtsprechung für die Telemedien-Angebote des öffentlich-rechtlichen Rundfunks.

Der Leitfaden bietet zunächst mit den Datenschutz-‚Basics' einen allgemeinen Überblick über die wichtigsten datenschutzrechtlichen Grundprinzipien, die bei der Planung und Umsetzung jedes neuen Angebots zu berücksichtigen sind. Sodann liegt der Fokus auf praxisrelevanten Einzelthemen. Am Ende eines jeden Kapitels findet sich ein Block „Empfehlungen für die Praxis", der zusammenfassend darstellt, worauf es bei der konkreten Realisierung von Angeboten ankommt.

Der Leitfaden möchte eine Orientierung bieten und die Telemedienverantwortlichen in den Rundfunkanstalten dabei unterstützen, datenschutzrelevante Themen zu erkennen, zu beurteilen und datenschutzkonform umzusetzen. Er soll jedoch nicht die Beratung mit dem/der zuständigen Datenschutzbeauftragten ersetzen, der/die in Zweifelsfragen immer hinzugezogen werden kann und sollte.

Regelmäßig sind neben dem Datenschutz auch andere rechtliche Aspekte zu beachten, die über die Justiziariate geklärt werden können (bspw. Fragen der Beschaffungsordnung und des Vergaberechts oder der personalvertretungsrechtlichen Mitbestimmung vor Einführung neuer IT-Systeme und -Anwendungen).



INHALT

LEGENDE

→ Verlinkung innerhalb des Berichts (Sprungmarke)

Link auf externe Website

DATENSCHUTZ–'BASICS' 5

Rechtlicher Rahmen 5
- DSGVO 5
- TTDSG 6

Definitionen 7
- Verantwortliche 7
- Personenbezogene Daten 9
- Verarbeitung 10
- Medienprivileg 16

DATENSCHUTZERKLÄRUNG 17

MINDERJÄHRIGEN-DATENSCHUTZ 23

AUFTRAGSVERARBEITUNG 28

CHATS, FOREN, GÄSTEBÜCHER, KOMMENTARFUNKTION 31

KONTAKTFORMULARE, NEWSLETTER 34

GEWINNSPIELE 37

VOTINGS 40

APPS 43

COOKIES, LOCAL-STORAGE-ELEMENTE & CO. 50

NUTZUNGSMESSUNG/ TRACKING 53

PERSONALISIERUNG 57

DRITTPLATTFORMEN 60

EMBEDDING VON FREMDINHALTEN 63

SOCIAL LOGIN 68

INSTANT MESSAGING 71

DATENSCHUTZ–'BASICS'

THEMEN

Rechtlicher Rahmen
→ **DSGVO**
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit

→ Medienprivileg

RECHTLICHER RAHMEN

DSGVO – EU UND EWR

Den wichtigsten rechtlichen Rahmen für die Verarbeitung personenbezogener Daten in Deutschland, wie auch in weiten Teilen Europas, bildet die seit 2018 geltende **Europäische Datenschutz-Grundverordnung** (im Folgenden: **DSGVO**). Dort sind **die grundlegenden Voraussetzungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten** innerhalb der Mitgliedstaaten der Europäischen Union (EU) und des Europäischen Wirtschaftsraumes (EWR) festgelegt.

DSGVO – DRITTLÄNDER

Gleichzeitig finden sich in der DSGVO dezidierte Vorgaben für eine rechtmäßige Übermittlung von personenbezogenen Daten an sog. „Drittländer" (d. h. Nicht-EU- bzw. Nicht-EWR-Staaten).
Regelmäßig relevant werden Drittstaatenübermittlungen für die Rundfunkanstalten z. B. bei Einführung von IT-Systemen oder -Anwendungen, bei denen Daten auf Servern in den USA gehostet werden. In erster Linie ist die Beauftragung Dritter, die ihren Sitz außerhalb des Europäischen Wirtschaftsraums haben, nur zulässig, wenn durch einen Angemessenheitsbeschluss der EU-Kommission festgestellt ist, dass in diesem Drittland ein mit der EU vergleichbares Datenschutzniveau vorzufinden ist (Art. 45 DSGVO). Derzeit gibt es für 14 Nicht-EWR-Staaten solche Angemessenheitsbeschlüsse, z. B. für das Vereinigte Königreich, die Schweiz, Kanada und Israel (**Adequacy decisions | EU-Kommission (europa.eu)**).

Für andere Drittländer, wie z. B. die USA, müssen seitens der Auftraggeber und der Auftragsverarbeiter durch sog. „geeignete Garantien" (Art. 46 DSGVO) andere Nachweise zur Einhaltung des angemessenen Datenschutzniveaus geführt werden. Dies geschieht in aktuellen Vertragsbeziehungen regelmäßig durch den Abschluss der von der EU-Kommission herausgegebenen sog. **Standardvertragsklauseln** (Art. 46 Abs. 2 lit. c DSGVO) zwischen den Auftraggebern – hier den Rundfunkanstalten – und den Auftragsverarbeitern (z. B. Microsoft). Der Wortlaut der Standardvertragsklauseln darf nicht verändert werden.
Zu beachten ist allerdings, dass es oftmals nicht genügt, dass die Vertragspartner die Standardvertragsklauseln einfach gegenseitig unterzeichnen. Die EuGH-Rechtsprechung verlangt vielmehr in jedem Einzelfall die vorherige Überprüfung, ob die verabredeten Standardvertragsklauseln in dem jeweiligen Drittland auch effektiv zur Anwendung kommen können und damit das zu fordernde EU-vergleichbare Datenschutzniveau eingehalten werden kann. Daran können aufgrund gesetzlicher und behördlicher Voraussetzungen in den Drittländern, wiederum insbesondere den USA, erhebliche Zweifel bestehen, wenn es dort z. B. weitgehende Zugriffsrechte von Straf- oder Geheimdienstbehörden auf Daten gibt, denen die Auftragsverarbeiter im Zweifelsfall nachkommen müssen.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ **TTDSG**

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung

Für die Rundfunkanstalten ist dies besonders relevant, wenn sie in den USA gehostete Cloud-Anwendungen einsetzen, bei denen personenbezogene Daten in die USA übermittelt werden. Eine Übermittlung von personenbezogenen Daten in Drittstaaten kann aber auch schon dann stattfinden, wenn die Server eines US-Cloud-Anbieters zwar im EWR-Raum stehen, Daten aber zu Wartungs- oder IT-Sicherheitszwecken aus dem EWR in die USA übermittelt werden.
In solchen Fällen müssen die Verantwortlichen zusätzliche vertragliche und/oder technische und organisatorische Maßnahmen (TOM) ergreifen, um ein mit europäischen Maßstäben vergleichbares Datenschutzniveau tatsächlich zu erreichen. Dabei werden von der EU zusätzliche technische Maßnahmen, wie z. B. hochgradige Verschlüsselungstechniken, als in erster Linie effektiv angesehen.

TTDSG

Im Zusammenhang mit der Gestaltung und dem Einsatz von Telemedien der Rundfunkanstalten hat das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG), welches am 1. Dezember 2021 in Kraft getreten ist, Bedeutung erlangt.

Zum einen enthält es besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien. Zum anderen regelt es aber auch den **Schutz von Endeinrichtungen der Nutzer:innen** (wie PC, Smartphone, Tablet etc.) hinsichtlich des Ablegens von Informationen in den Geräten oder des Auslesens von Informationen aus den in ihren Geräten vorhandenen Informationen **und zwar unabhängig davon, ob es sich dabei um Daten handelt, die Personenbezug aufweisen oder nicht (§ 25 TTDSG).**

Grundsätzlich sind danach entsprechende Zugriffe auf Endeinrichtungen nur noch zulässig, wenn die betroffenen Nutzer:innen zuvor informiert und aktiv eingewilligt haben. Die Anforderungen an diese Einwilligung entsprechen den Vorgaben der DSGVO. (→ **Rechtmäßigkeit der Verarbeitung**).
§ 25 Abs. 2 TTDSG nennt aber auch Ausnahmen von der Pflicht zur Einholung einer Einwilligung. Für die Rundfunkanstalten wird insbesondere der Ausnahmefall relevant werden, wonach die Einwilligung der Nutzer:innen entbehrlich ist, *„... wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann“*.

Dies kann z. B. den Bereich der Messung von Nutzerverhalten betreffen (→ **Nutzungsmessung/Tracking**).

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Defintionen
→ **Verantwortliche**
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit

→ Medienprivileg

VERANTWORTLICHE

Nach der Definition der DSGVO (Art. 4 Nr. 7) ist **„Verantwortlicher“** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Der Verantwortliche hat die Einhaltung der Vorgaben der DSGVO sicherzustellen und die von ihm eingesetzten Mitarbeiter:innen entsprechend auf die Einhaltung der Datenschutzvorschriften zu verpflichten, zu sensibilisieren und zu unterweisen. Auch im Falle der Auslagerung einer Datenverarbeitungsaufgabe oder -maßnahme auf einen externen Auftragnehmer verbleibt die datenschutzrechtliche Verantwortlichkeit beim Auftraggeber, hier also der Rundfunkanstalt. Sie muss dem Auftragnehmer entsprechende vertragliche Weisungen zur Einhaltung des Datenschutzes erteilen und entsprechende Nachweise über die Bereitstellung sog. „technischer und organisatorischer Maßnahmen“ (Art. 32 DSGVO) von ihm verlangen (→ **Auftragsverarbeitung**).

Nicht selten kommt es aber auch vor, dass zwei oder **mehrere Verantwortliche** die Mittel und Zwecke einer Verarbeitung personenbezogener Daten gemeinsam festlegen (sog. **„Joint Controller“**).

In solch einem Fall haben sie in einem Vertrag festzulegen, wer von ihnen welche Aufgaben des Datenschutzes im Rahmen ihres Vertragsverhältnisses übernimmt (Art. 26 Abs. 1 S. 2 DSGVO).
Innerhalb des öffentlich-rechtlichen Rundfunks ist dies z. B. beim Betrieb von Gemeinschaftseinrichtungen der Fall.

Für Joint-Controller-Konstellationen mit außereuropäischen Vertragspartnern sind die speziell dafür von der EU-Kommission herausgegebenen EU-Standardvertragsklauseln abzuschließen.

Prominentes praktisches Beispiel für eine durch die Rechtsprechung festgestellte Joint-Controller-Konstellation ist das Betreiben einer **Facebook-Fanpage**. In seinem Urteil vom 5. Juni 2018 hat der EuGH festgestellt, dass Facebook und Fanpage-Betreiber für bestimmte bei Facebook stattfindende personenbezogene Datenverarbeitungen jedenfalls teilweise gemeinsam verantwortlich sind (hier: Auswertungen von Nutzerverhalten seitens Facebook, die den Fanpage-Betreibern in eingeschränkt aggregierten Statistiken zur Verfügung gestellt werden, die sog. Facebook-Insights). Aus diesem Grund haben die Rundfunkanstalten darauf hinzuwirken, mit Facebook einen Joint-Controller-Vertrag abzuschließen. Facebook allerdings sieht keine Veranlassung zum Abschluss eines solchen Vertrages bzw. betrachtet seine mit Blick auf das EuGH-Urteil ergänzten Nutzungsbedingungen als ausreichend. Die Rundfunkdatenschutzaufsichten

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ **Verantwortliche**
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit

→ Medienprivileg

verlangen zusätzlich zumindest eine gegenüber den Nutzer:innen transparente Begründung der Rundfunkanstalten (z. B. innerhalb der Datenschutzerklärungen auf den Websites der Häuser), warum sie Facebook-Fanpages einsetzen, um ihren staatsvertraglichen Auftrag zu erfüllen. Die Rundfunkanstalten müssen die Nutzer:innen der Fanpages zudem über die von Facebook eingesetzten Cookies, die damit verbundene Datenauswertung sowie den Datentransfer in ein Drittland informieren (→ **Drittplattformen** und → **Datenschutzerklärung**).
Die in dem Urteil getroffenen Aussagen dürften aber auch für andere Drittplattformen gelten, die die Rundfunkanstalten nutzen, soweit von dort ähnliche Auswertungen wie bei den Facebook-Insights an die Anstalten übermittelt werden.

Wichtig für die Rundfunkanstalt ist – ebenso wie bei der Beauftragung von Dritten – die sorgfältige Auswahl der anderen Joint Controller, mit denen sie eine gemeinsame Datenverarbeitungsaufgabe durchführen will. Denn im Fall der Verletzung von Datenschutzrechten (z. B. ein ‚Datenleck' größeren Ausmaßes bei einem Vertragspartner) haften nach außen zunächst einmal alle Joint Controller gemeinsam. In einem aufwändigen Prozess werden erst im Nachgang die jedem einzelnen Vertragspartner zuzuweisenden Verantwortungsteile geklärt. Auch wenn eine Rundfunkanstalt dann nur ein kleiner Teil der Verantwortung trifft, kann dennoch ein ggf. hoher Imageschaden für sie die Folge sein.

Abgrenzungsfragen im Zusammenhang mit den Verantwortlichkeiten der an Datenverarbeitungsprozessen Beteiligten sind oftmals komplex. Bezüge zu Drittländern bieten aufgrund der gegebenenfalls einzubindenden „Standardvertragsklauseln", wie oben dargelegt, zusätzliche Schwierigkeiten. Für die rechtskonforme Gestaltung solcher Konstellationen können und sollten daher die Datenschutzbeauftragten beratend hinzugezogen werden.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ **Personenbezogene Daten**
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit

→ Medienprivileg

PERSONENBEZOGENE DATEN

Im Bereich der Telemedien kommen die Regelungen des Datenschutzrechts in erster Linie dort zur Anwendung, wo personenbezogene Daten von Nutzer:innen der Angebote verarbeitet werden. Dies können bspw. Angebote auf eigenen Websites oder in eigenen Apps der Rundfunkanstalten sein oder auch solche auf Drittplattformen (wie z. B. Facebook und Twitter).

Die DSGVO definiert „personenbezogene Daten“ (Art. 4 Nr. 1 DSGVO) als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person – auch „betroffene Person“ genannt – beziehen. Als identifizierbar sind natürliche Personen anzusehen, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer oder Online-Kennung (bspw. eine IP-Adresse zu Standortdaten oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind), identifiziert werden können.

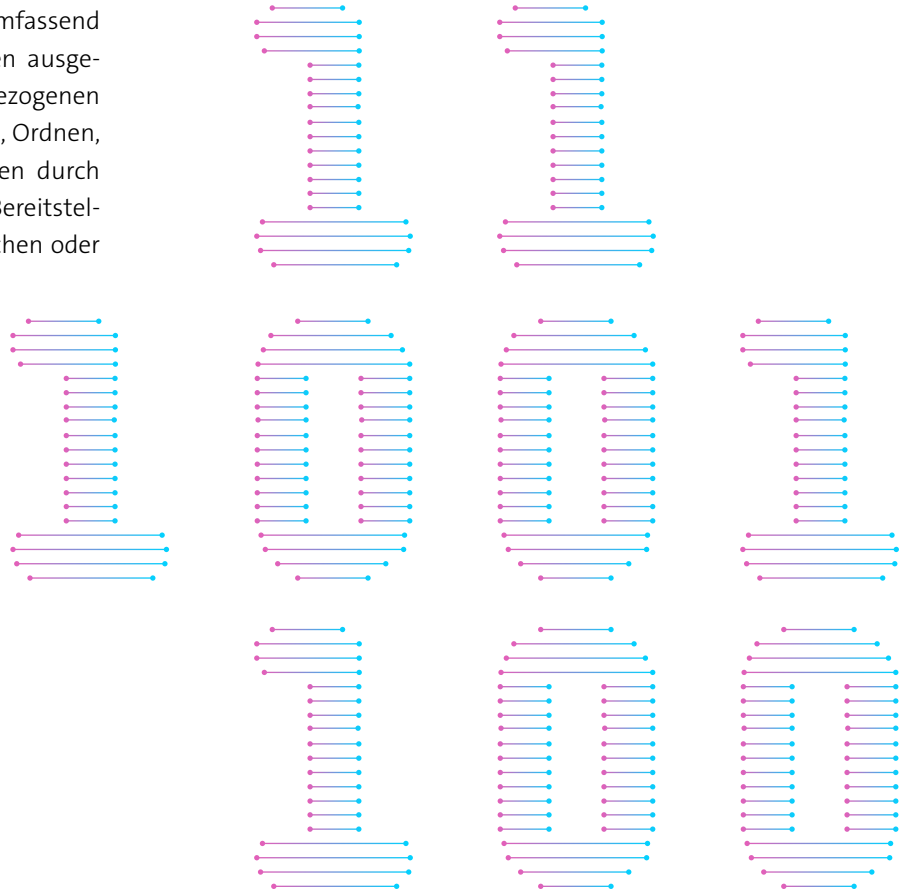
THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ **Verarbeitung**
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ Medienprivileg

VERARBEITUNG

Mit Verarbeitung meint die DSGVO (Art. 4 Nr. 2) umfassend jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten, wie bspw. das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Verändern, Auslesen, Abfragen, Offenlegen durch Übermittlung, Verbreiten oder eine andere Form der Bereitstellung, das Abgleichen, Verknüpfen, Einschränken, Löschen oder das Vernichten von personenbezogenen Daten.



THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- **Rechtmäßigkeit**
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ Medienprivileg

RECHTMÄSSIGKEIT DER VERARBEITUNG

Die Verarbeitung personenbezogener Daten darf nur erfolgen, wenn es dafür eine gesetzliche Grundlage gibt. Die DSGVO sieht einen abschließenden Katalog von **Rechtsgrundlagen für die Verarbeitung vor (Art. 6 Abs. 1 S. 1 lit. a bis f DSGVO)**:

Besonders relevant für die Verarbeitung personenbezogener Daten in Telemedien der Rundfunkanstalten ist die Rechtsgrundlage ***„Wahrnehmung einer Aufgabe […], die im öffentlichen Interesse liegt […], die dem Verantwortlichen übertragen wurde“*** (Art. 6 Abs. 1 S. 1 lit. e DSGVO). Die Rundfunkanstalten sind mit solchen öffentlich-rechtlichen Aufgaben – Veranstaltung und Verbreitung von Rundfunk und Telemedien – durch die für sie geltenden Staatsverträge betraut. Z. B. können → **Nutzungsmessung/Tracking** auf Websites oder in Apps als Bestandteil des staatsvertraglichen Programmauftrags unter diese Rechtsgrundlage gefasst werden.

Oftmals überschneidet sich die Anwendbarkeit dieser Rechtsgrundlage mit weiteren Grundlagen, nämlich der ***„Erfüllung einer rechtlichen Verpflichtung […], der der Verantwortliche unterliegt“ (Art. 6 Abs. 1 S. 1 lit. c DSGVO) oder der „Verarbeitung […] zur Wahrung der berechtigten Interessen des Verantwortlichen […], sofern nicht die Interessen […] der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen […]“*** (Art. 6 Abs. 1 S. 1 lit. f DSGVO). Letztere kann z. B. für die Speicherung von Log-Daten beim Besuch einer Webseite der Rundfunkanstalt herangezogen werden.

Den genannten Rechtsgrundlagen ist gemeinsam, dass die auf sie gestützten Verarbeitungen erforderlich sein müssen, um die Aufgabe bzw. die Pflicht zu erfüllen oder das berechtigte Interesse wahrzunehmen. Damit ist in diesen Rechtsgrundlagen die Voraussetzung einer Interessenabwägung für jeden konkreten Einzelfall verankert. Die datenschutzrechtliche Zulässigkeit von personenbezogenen Datenverarbeitungen lässt sich in diesen Fällen also nicht pauschal beurteilen, sondern ist immer auch mit den ggf. entgegenstehenden Datenschutzinteressen der Betroffenen abzuwägen. Zu den erforderlichen Einzelfallprüfungen kann und sollte in Zweifelsfällen der/die Datenschutzbeauftragte beratend hinzugezogen werden.

Relevant sind im Telemedienbereich auch die **Rechtsgrundlagen „Einwilligung“ (Art. 6 Abs. 1 S. 1 lit. a DSGVO)**, z. B. bei der Bestellung von Newslettern durch die Nutzer:innen oder **„Vertragserfüllung“ (Art. 6 Abs. 1 S. 1 lit. b DSGVO)**, z. B. bei einem → **Gewinnspiel**.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ Medienprivileg

AN DIE RECHTMÄSSIGKEIT DER EINWILLIGUNG WERDEN VON DER DSGVO VERSCHIEDENE EINZELVORAUSSETZUNGEN GEKNÜPFT (ART. 7 DSGVO), INSBESONDERE:

> Der Text der Einwilligungserklärung muss den Nutzer/die Nutzerin klar und allgemein verständlich über die zu verarbeitenden personenbezogenen Daten und den vorgesehenen Zweck der Verarbeitung informieren.

> Der Einwilligungstext muss klar und eindeutig formuliert sein, so dass die Nutzenden erkennen können, was sie hier erklären („Ich willige ein, dass …"; „Ich bin einverstanden, dass …").

> Es muss sich um eine bewusste Erklärung handeln (Opt-In). Diese kann z. B. im Wege eines Häkchens in einer Checkbox abgegeben werden. Zustimmung durch vorangekreuzte Einwilligungstexte oder nur mit einer Streich-/Abwahlmöglichkeit versehene ‚vorgegebene' Zustimmungen (Opt-Out) genügen nicht.

> Sollen besonders sensible persönliche Daten (Art. 9 DSGVO) erhoben und verarbeitet werden, sind die jeweils Nutzenden darüber im Zuge ihrer Einwilligung gesondert zu unterrichten. Dies ist z. B. der Fall bei:
- Angaben über die ethnische Herkunft;
- politischen Meinungen;
- religiösen und philosophischen Überzeugungen;
- Daten zu Gesundheit und Sexualleben;
- Daten über Straftaten.

> Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt, muss die Einwilligung protokolliert bzw. dokumentiert werden.

> Die Einwilligung muss jederzeit in einfacher Weise von den einzelnen Nutzenden widerrufbar sein. Sie sind jeweils vorab über ihr Widerrufsrecht zu informieren.

Die datenschutzrechtliche Einwilligung zu einer konkreten Datenverarbeitung sollte deutlich getrennt werden von den generell informierenden Datenschutzhinweisen in einem Telemedienangebot.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ Medienprivileg

ZWECKBINDUNG

Jede Verarbeitung personenbezogener Daten darf nur für festgelegte, eindeutige und legitime Zweck erfolgen (Art. 5 Abs. 1 lit. b DSGVO). Eine Verwendung der Daten für andere Zwecke ohne Wissen und Einverständnis der jeweiligen Nutzer:innen ist ebenfalls grundsätzlich nicht zulässig. Beispiel: Abonnent:innen eines Newsletters für eine Klassik-Radiowelle dürfen nicht ungefragt weitere Newsletter zugesandt bekommen.

TRANSPARENZ

Das Grundrecht auf informationelle Selbstbestimmung verlangt: Die einzelne Person soll wissen, wer was wann und bei welcher Gelegenheit über ihn weiß. Dieses Transparenzprinzip wirkt sich auch in umfangreichen **Rechenschafts- sowie Informations- und Auskunftspflichten aus (Art. 5 Abs. 2 DSGVO, Art. 13 ff. DSGVO)**, die die Rundfunkanstalt gegenüber den Nutzer:innen ihrer Angebote hat, soweit sie dabei deren personenbezogene Daten verarbeitet.

Als Anbieter von Websites oder Apps sind die Rundfunkanstalten insbesondere verpflichtet, die Nutzer:innen 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 (→ **Datenschutzerklärung**).

Jede nutzende Person, deren personenbezogene Daten durch die Rundfunkanstalt erhoben und verwendet werden, hat zudem das Recht, Auskunft über die zu ihr gespeicherten Daten zu verlangen. Unter bestimmten Voraussetzungen kann sie zudem die **Berichtigung, Löschung oder Sperrung** von Daten verlangen.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ Medienprivileg

DATENMINIMIERUNG

Es sollen immer so wenig personenbezogene Daten wie möglich für den konkret festgelegten Zweck abgefragt werden (Art. 5 Abs. 1 lit. c DSGVO). Dabei hilft die Kontrollfrage: *„Benötigen wir diese Daten tatsächlich zur Zweckerfüllung?“*

Diesem Ziel kann auch eine Pseudonymisierung oder Anonymisierung von Daten dienen. Bei der **Pseudonymisierung** wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (i. d. R. eine mehrstellige Buchstaben- oder Zahlenkombination, auch Hash genannt) ersetzt, um die Identifizierung des Betroffenen zu verhindern oder zumindest wesentlich zu erschweren. Dabei ist eine Wiederherstellbarkeit der Identifizierbarkeit aber noch gegeben. In Abgrenzung dazu ist die **Anonymisierung** das dauerhafte und nicht mehr umkehrbare Verändern personenbezogener Daten derart, dass diese Daten überhaupt nicht mehr einer Person zugeordnet werden können. Soweit es der Rundfunkanstalt technisch möglich und im Rahmen der Zweckerfüllung zumutbar ist, sollte sie für ihre Telemedienangeboten Verfahren der Anonymisierung oder Pseudonymisierung nutzen.

Auch datenschutzfreundliche Technikgestaltung **„Privacy by Design“** und datenschutzfreundliche Voreinstellungen **„Privacy by Default“ (Art. 25 DSGVO)** können bereits in der Entstehungs- und Entwicklungsphase von Telemedienangeboten helfen, dem Grundsatz der Datenminimierung Rechnung zu tragen. So kann Datenschutz von vorneherein in die Gesamtkonzeption einbezogen werden, anstatt Datenschutzprobleme im Nachhinein mühsam und mit viel Zeitaufwand durch Korrekturmaßnahmen zu beheben.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ Medienprivileg

SPEICHERBEGRENZUNG

Sobald die personenbezogenen Daten nicht mehr zu dem ursprünglich angegebenen Zweck benötigt werden, müssen sie grundsätzlich gelöscht werden (Art. 5 Abs. 1 lit. e i. V. m. Art. 17 DSGVO). Das gleiche gilt im Falle des Widerrufs einer Einwilligungserklärung in die Datenverarbeitung durch die jeweiligen Nutzer:innen. Zu berücksichtigen sind allerdings gesetzliche Aufbewahrungspflichten (z. B. nach den Vorgaben der Abgabenordnung oder des Handelsgesetzbuches).

Auch verlangt die DSGVO, dass in einem Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen (Art. 30 DSGVO) Angaben zu den Löschfristen für die jeweils verarbeiteten Datenkategorien gemacht werden. Ein Konzept, das die Zeitpunkte bzw. die Kriterien für die Löschung von personenbezogenen Daten vorsieht, sollte daher bereits in der Planungsphase jedes neuen Telemedienangebots mitentwickelt werden.

DATENSICHERHEIT

IT-Systeme sind aufgrund ihrer Komplexität anfällig für Fehler, über die z. B. Unbefugte an Daten gelangen können. Gleichzeitig werden auch die Angriffe auf technische Systeme immer häufiger und ausgefeilter. Die Rundfunkanstalten haben daher unter Einbindung der IT-Sicherheitsbeauftragten und/oder der zuständigen Fachabteilungen für ihre Telemedienangebote, in denen sie personenbezogene Daten ihrer Nutzer:innen verarbeiten, **technische und organisatorische Maßnahmen zu ergreifen (Art. 5 Abs. 1 lit. f, Art. 24, Art. 32 DSGVO)**, um diese Daten gegen unbefugte und unsachgemäße Verwendung, wie z. B. Offenlegung oder Datendiebstahl, Verfälschung oder Verlust zu schützen (Schutz von Vertraulichkeit, Integrität und Verfügbarkeit der Daten). Insbesondere sind ein IT-Sicherheitskonzept und ein Berechtigungskonzept, welches die Zugriffe regelt, zu erstellen.

THEMEN

Rechtlicher Rahmen
→ DSGVO
→ TTDSG

Definitionen
→ Verantwortliche
→ Personenbezogene Daten
→ Verarbeitung
- Rechtmäßigkeit
- Zweckbindung
- Transparenz
- Datenminimierung
- Speicherbegrenzung
- Datensicherheit
→ **Medienprivileg**

MEDIENPRIVILEG

Im Bereich der **Verarbeitung personenbezogener Daten für journalistische Zwecke** gelten die umfangreichen Informations- und Dokumentationspflichten, Auskunfts- und Widerrufsrechte für die Betroffenen nach DSGVO nicht (sog. Medienprivileg, Art. 85 DSGVO). Gleichwohl sind die speziellen Regelungen in §§ 12, 23 Medienstaatsvertrag (z. B. Recht auf Gegendarstellung) zu beachten.

Geschützt und privilegiert sind die Medien, wenn und soweit sie mit ihren Tätigkeiten die Weitergabe von Informationen, Meinungen und Vorstellungen an die Öffentlichkeit bezwecken. Erfasst sind davon die Recherche, Redaktion, Veröffentlichung, Dokumentation und Archivierung. Starre Grenzen des Medienprivilegs sind nicht abgesteckt. Im entsprechenden Erwägungsgrund Nr. 153 zur DSGVO heißt es vielmehr:
„ … Um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen, müssen Begriffe wie Journalismus, die sich auf diese Freiheit beziehen, weit ausgelegt werden.“

Die mit Tätigkeiten zu journalistischen Zwecken befassten Personen sind dem Datenschutz insoweit verpflichtet, als es ihnen untersagt ist, personenbezogene Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Sie sind vor Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten, das auch nach Beendigung ihrer Tätigkeit fortbesteht.

Die Verantwortlichen haben auch im Bereich der journalistischen Verarbeitung geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten festzulegen und umzusetzen (→ **Datensicherheit**).

DATENSCHUTZERKLÄRUNG

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen
für die Praxis
- Form
- Inhalt

Websites und Apps verarbeiten eine Vielzahl von Daten ihrer Nutzer:innen. In der nach der DSGVO vorgeschriebenen Datenschutzerklärung für ein Onlineangebot bzw. eine App muss über Art und Umfang der Datenverarbeitung aufgeklärt werden. Zugleich wahrt die Datenschutzerklärung die Datensouveränität der Nutzer:innen und schafft Vertrauen zwischen ihnen und der Rundfunkanstalt. Datenschutzerklärungen müssen vollständig, transparent und verständlich sein.

WAS SAGT DER DATENSCHUTZ?

Das Datenschutzrecht verpflichtet die Rundfunkanstalten, die Nutzer:innen ihrer Onlineangebote und Apps 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.

In der Datenschutzerklärung wird darüber informiert, wie die Rundfunkanstalt die personenbezogenen Daten ihrer Nutzer:innen (aufgrund gesetzlicher Befugnisse) verarbeitet. Die Nutzer:innen müssen die Datenschutzerklärung nicht ausdrücklich akzeptieren. Die Möglichkeit der Kenntnisnahme der Datenschutzerklärung reicht aus. Die Veröffentlichung der Datenschutzerklärung ist von der Einholung einer informierten Einwilligung zu unterscheiden. Einwilligungen müssen eingeholt werden, um Daten in einer nicht schon im Gesetz vorgesehenen Art und Weise nutzen oder zu einem weitergehenden Zweck verarbeiten zu können (z. B. Abonnement eines Newsletters).

Datenschutzerklärungen sind auch von einem Impressum zu unterscheiden. Die Impressumspflicht ist eine allgemeine medienrechtliche Pflicht: Besucher:innen einer Website sollen wissen können, wer für eine Website medienrechtlich verantwortlich ist.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- Form
- Inhalt

EMPFEHLUNGEN FÜR DIE PRAXIS

FORM: ALLGEMEIN VERSTÄNDLICH, LEICHT AUFFINDBAR UND JEDERZEIT ABRUFBAR

Die Datenschutzerklärung muss allgemein verständlich, präzise und transparent formuliert sein. Technische oder juristische Fachbegriffe und Formulierungen sollen daher nach Möglichkeit vermieden oder erläutert werden.

Bereits auf der Startseite der Website einer Rundfunkanstalt muss ein eindeutiger, leicht auffindbarer Link auf die Datenschutzerklärung enthalten sein. Zudem muss 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, die sich explizit an Minderjährige richten, sollte neben der Datenschutzerklärung für ihre Erziehungsberechtigten zusätzlich eine Datenschutzerklärung in einer für Kinder und Jugendliche verständlichen Form bereitgestellt werden (→ **Minderjährigen-Datenschutz**).

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen
für die Praxis
- Form
- Inhalt

INHALT: WAS MUSS ENTHALTEN SEIN?

Eine Datenschutzerklärung muss grundsätzlich für das gesamte Onlineangebot formuliert werden. Ergänzende Hinweise zum Datenschutz auf einzelnen Seiten eines Onlineangebots (z. B. spezifische Hinweise zu Programmaktionen, Gewinnspielen, Umfragen) sind ggf. nötig. Die erforderlichen Angaben richten sich nach den spezifischen Angeboten und Funktionen der Website. Zu beachten ist zudem, dass unterschiedliche Ausspielwege eines Onlineangebots abweichende Datenschutzerklärungen notwendig machen können (z. B. weil Apps andere Daten verarbeiten können, als die entsprechende Website).

Grundsätzlich gilt es, die Nutzer:innen über die Art, den Umfang und die Zwecke der Erhebung und die Verwendung personenbezogener Daten transparent zu unterrichten. Je mehr Daten von den Nutzer:innen erhoben werden und je sensibler die Daten sind, desto ausführlicher muss die Unterrichtung sein.

ZU INFORMIEREN IST ÜBER

- **den Namen und die Kontaktdaten des/der Verantwortlichen,**
- **Kontaktdaten des/der Datenschutzbeauftragten,**
- **Zwecke und Rechtsgrundlagen der Datenverarbeitung,**
- **den Einsatz von Cookies und Local-Storage-Elementen,**
- **die Speicherdauer der Daten (mindestens die Kriterien für die Festlegung dieser Dauer),**
- **bei Einbindung von Drittanbietern (technisch, gestaltend oder redaktionell) über die Weitergabe von personenbezogenen Daten,**
- **evtl. Übermittlung der Daten in Länder außerhalb der EU,**
- **die Rechte der Nutzer:innen (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragung),**
- **das Beschwerderecht bei der zuständigen Datenschutzaufsichtsbehörde,**
- **etwaige Besonderheiten bei der Verbreitung des Angebots,**
- **besondere Umstände der Datenverarbeitung bei unterschiedlichen Ausspielwegen, z. B. bei Apps und HbbTV.**
- **das Widerrufsrecht bei Einwilligungen**
- **berechtigte Interessen, auf die eine Datenverarbeitung gestützt wird**
- **ggf. die Kategorien von Empfängern der personenbezogenen Daten**

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen
für die Praxis
- Form
- Inhalt

IM EINZELNEN:

Namen und Kontaktdaten des/der Verantwortlichen
Dies ist die jeweilige Rundfunkanstalt, der/die Intendant:in. Die postalische Anschrift und eine E-Mail-Adresse sind zu benennen.

Kontaktdaten des/der Datenschutzbeauftragten
Der/die Datenschutzbeauftragte der Rundfunkanstalt, die postalische Anschrift und eine E-Mail-Adresse sind anzugeben.

Zwecke und Rechtsgrundlagen der Datenverarbeitung
Es ist darzulegen, warum welche Daten bei der Nutzung des Angebots erhoben werden und auf welcher Rechtsgrundlage dies geschieht. Hinsichtlich der Rechtsgrundlagen empfiehlt sich, die Beratung der/des Datenschutzbeauftragten hinzuzuziehen.
Zu erläutern ist, was beim Aufruf und bei der Nutzung des Onlineangebots bzw. der App passiert. Dazu gehört etwa die Benennung der Server-Log-Daten (Datum und Uhrzeit des Besuches, die verwendete IP-Adresse, Browsertyp/-version und Betriebssystem; besuchte Webseiten und Herkunftsseite); Gerätedaten; Standortdaten o. Ä.

Ebenso kann bereits hier über die Datenverarbeitung bei Kontaktaufnahme (z. B. Kontaktformular), beim Abonnieren von Newslettern, bei Gewinn- und Tippspielen sowie bei Umfragen oder Votings informiert werden. (→ **„Besonderheiten des Angebots“**). Es empfiehlt sich überdies, bereits an dieser Stelle über die Verwendung von Daten zur Nutzungsmessung aufzuklären, zu der ggf. auch Cookies oder Identifier eingesetzt werden, über die gesondert informiert werden muss. Hierzu kann auch der Einsatz von Analysediensten zählen. Jedenfalls ist darzulegen, welche Daten wozu genutzt werden.

Einsatz von Cookies
Welche Cookies oder Identifier werden genutzt, welche Daten werden dabei wozu durch die Rundfunkanstalt oder Dritte genutzt? Ggf. ist eine Einwilligung für das Setzen von Cookies einzuholen (→ **Cookies, Local-Storage-Elemente & Co.**).

Speicherdauer der Daten
Die Nutzer:innen müssen wissen, wie lange ihre Daten gespeichert werden. Zumindest sind die Kriterien für die Festlegung der Speicherfristen anzugeben.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen
für die Praxis
- Form
- Inhalt

Einbindung von Dienstleistern oder Drittinhalten
Über den Einsatz von Auftragsverarbeitern bzw. Kategorien von Auftragsverarbeitern muss ebenfalls aufgeklärt werden. Auch muss ggf. auf eingebettete Inhalte Dritter hingewiesen werden. (→ **Embedding von Fremdinhalten**).

Eventuelle Übermittlung der Daten in Länder außerhalb der EU
Werden, insbesondere durch eingebundene Auftragsverarbeiter, personenbezogene Daten in Länder außerhalb des Geltungsraums der DSGVO übermittelt (→ **Auftragsverarbeitung**), muss dies in der Datenschutzerklärung mitgeteilt werden. Zugleich ist darzulegen, wie die Daten dabei geschützt werden, welche Garantien ggf. zum Schutz der Daten bestehen und wie eine Kopie dieser Garantien zu erhalten ist.

Rechte der Nutzer:innen (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragung)
Es sind Ausführungen zu den sog. Betroffenenrechten wie Auskunft, Berichtigung und Löschung zu machen. Zugleich ist anzugeben, gegenüber welcher Stelle die Ansprüche geltend zu machen sind. Dabei sollte eine einfache Möglichkeit der Kontaktaufnahme (z. B. via E-Mail und Telefon) angeboten werden.

Beschwerderecht bei einer Datenschutzaufsichtsbehörde
Die zuständige Aufsichtsbehörde und die Kontaktdaten sind anzugeben. Bei gemeinschaftlichen Angeboten ist darauf hinzuweisen, wer nach dem Federführungsprinzip zuständige Aufsichtsbehörde ist.

Besonderheiten des Angebots
Sind Bestandteile des Angebots bspw. Gewinnspiele, Foren, Kommentarfunktionen, Newsletter-Abonnements, Social-Media-Funktionen oder andere Tools, so ist deren Beschreibung einschließlich der dafür erforderlichen Daten notwendig. Gleiches gilt auch für personalisierte Angebote. Bei diesen Funktionen ist regelmäßig das Einholen einer Einwilligung der Nutzer:innen erforderlich. Sie sind auf die Möglichkeit des Widerrufs einer erteilten Einwilligung hinzuweisen, inklusive einer einfachen Kontaktmöglichkeit (z. B. per E-Mail). Sollte das Onlineangebot oder einzelne Funktionen unter Pseudonym genutzt werden können, sind auch Ausführungen dazu zu tätigen.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen
für die Praxis
- Form
- Inhalt

Besondere Ausspielwege

Besondere Ausspielwege (z. B. Apps von Telemedienangeboten, HbbTV) können zu unterschiedlichen Datenverarbeitungen führen. In der Datenschutzerklärung für das Onlineangebot bzw. für die App ist daher entsprechend darauf hinzuweisen.
Die Rundfunkanstalt sollte über die Auftritte auf Social-Media-Plattformen und anderen Drittplattformen informieren. Dazu gehört der Hinweis auf die Datenschutzrichtlinie der jeweiligen Drittplattformen und die ggf. teilweise eigene Verantwortung der Anstalten für die Datenverarbeitung auf den Drittplattformen (→ **Drittplattformen**).

Bei der Verbreitung eines Angebots über Apps ist auf diese spezifische Ausspielform einzugehen:
> Auf welche Daten wird zugegriffen?
> Weshalb erfolgt wann und wozu ein Zugriff?

Vor der Veröffentlichung einer Datenschutzerklärung empfiehlt es sich, Rücksprache mit den zuständigen Datenschutzbeauftragten zu halten, um die Erfüllung aller Anforderungen prüfen zu lassen.

MINDERJÄHRIGEN-DATENSCHUTZ

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- 13 – 16-Jährige
- Unter 13-Jährige
- Kinderfreundliche Datenschutzerklärung

Die Rundfunkanstalten wenden sich mit ihren Telemedienangeboten auch an Kinder und Jugendliche, also an Minderjährige. Beispiele für Angebote bzw. Bestandteile von Angeboten, bei denen personenbezogene Daten von Minderjährigen erhoben werden, sind Newsletter, Chats, Gewinnspiele und Mitmachaktionen sowie Apps und Personalisierungen. 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 von ihnen abgefragt werden. Die beim Besuch einer Seite ohnehin anfallende IP-Adresse ist notwendig zur Bereitstellung des Dienstes und insoweit unkritisch.

Sobald persönliche Daten, zum Beispiel zu Personalisierungszwecken, erhoben werden, muss, wie bei Erwachsenen auch, eine Einwilligung eingeholt werden. Ab dem 16. Lebensjahr ist dies unproblematisch: Jugendliche können wie Volljährige behandelt werden. Im Grundsatz gilt, dass bei einem Alter unter 16 Jahren die Einwilligung der Träger der elterlichen Verantwortung einholt werden muss. Im Ausnahmefall und wenn das Risiko der Datenverarbeitung nur gering ist, kann die Einwilligung auch ab dem 13. Lebensjahr von den Jugendlichen selbst erklärt werden. Dies ist allerdings nur möglich, wenn sie verstehen können, welche Konsequenzen die jeweilige Datenverarbeitung für sie haben kann, man spricht dann von Einsichtsfähigkeit. Dies ist nur anhand der jeweiligen Konstellation zu beurteilen. ‚Auf der sicheren Seite' ist man also immer dann, wenn bis zur Vollendung des 16. Lebensjahrs die Einwilligung der Eltern eingeholt wird.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- 13 – 16-Jährige
- Unter 13-Jährige
- Kinderfreundliche Datenschutzerklärung

EMPFEHLUNGEN FÜR DIE PRAXIS

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 wie Erwachsene behandelt werden. Für sie gelten keine Besonderheiten. Sie können ohne Mitwirkung der Eltern in eine Datenverarbeitung rechtswirksam einwilligen; ebenso können sie ihre Einwilligung auch jederzeit selbst widerrufen. Im Übrigen gelten sämtliche datenschutzrechtlichen Vorgaben und Grundsätze (Datenminimierung, Zweckbindung, Transparenz, Löschung usw. – → **Datenschutz-‚Basics'**).

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- 13 – 16-Jährige
- Unter 13-Jährige
- Kinderfreundliche Datenschutzerklärung

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 damit einhergehenden Verständnis der Tragweite der Entscheidung in die Datenpreisgabe ab. Maßgeblich ist die am konkreten Fall und den anzusprechenden Jugendlichen zu messende Einsichtsfähigkeit. Insofern kommt es in dieser Altersgruppe immer auf den Einzelfall an.

Es ist dabei zu berücksichtigen, dass Jugendliche in dieser Altersgruppe mit Computern und Social Media aufgewachsen sind und regelmäßig schon Erfahrungen im Umgang mit dem Internet gesammelt haben.

Entscheidend ist auch der Zweck der Datenabfrage. Danach sollte es für Kinder und Jugendliche beispielsweise möglich sein, einen Newsletter der Lieblings-Website zu abonnieren oder sich auf einer Lernplattform zu registrieren.
Ab Vollendung des 13. Lebensjahrs kann von einer Einsichtsfähigkeit ausgegangen werden, wenn transparent und altersgerecht über die Art und den Zweck der Datenverarbeitung aufgeklärt wird und kein Risiko für die Jugendlichen aufgrund der nur sehr geringfügigen Datenerhebung besteht.

Es wird empfohlen, z. B. einen spielerischen Zugang zu wählen und damit die Einsichtsfähigkeit ‚abzuprüfen'. Die Teilnahme an einem Datenschutzspiel mit Lösung der damit verbundenen Aufgaben kann die Voraussetzung für die Nutzung eines Angebotes sein.

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit usw. (→ **Datenschutz-‚Basics'**).

WICHTIG:
Ohne datenschutzrechtliches Risiko kann in dieser Altersgruppe jedoch nur mit Einholung der Einwilligung der Eltern gearbeitet werden.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen
für die Praxis
- 13 – 16-Jährige
- Unter 13-Jährige
- Kinderfreundliche
Datenschutzerklärung

ACHTUNG BEI KINDERN UNTER 13 JAHREN: EINWILLIGUNG DER ELTERN ERFORDERLICH

Bei Kindern unter 13 Jahren muss eine Einwilligung der Eltern vorliegen. 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. Hier müssen Kinder die E-Mail-Adresse der Eltern angeben und diese müssen dann der Datenverwendung zustimmen. Dieses Verfahren ist nicht vollständig sicher, weil es durch die Minderjährigen umgangen werden kann. Die Sicherheit kann erhöht werden, indem im Rahmen der per E-Mail gesandten Einwilligungseinholung eine Frage gestellt wird, die ein Kind in der Regel nicht beantworten kann.

Der Weg zu einer Einwilligung der Eltern kann folgendermaßen aussehen:

1. Kind registriert sich selbständig mit eigener E-Mail-Adresse und Passwort
2. Kind muss E-Mail-Adresse eines Elternteils hinterlegen
3. Elternteil wird per E-Mail auf den Vorgang hingewiesen und erhält einen Link zu einem Eingabeformular
4. Elternteil öffnet das Eingabeformular und
   a) hinterlegt dort ein eigenes Passwort,
   b) altersverifiziert sich mittels Personalausweis,
   c) kann die Datenschutzerklärungen einsehen und die Einwilligung abgeben,
   d) Kind-Profil wird freigeschaltet,
   e) Kind wird per E-Mail darüber informiert.
6. Kind kann sich Nickname vergeben
7. Nickname wird redaktionell geprüft und freigegeben

Im Hinblick auf die praktischen Schwierigkeiten bei der Einwilligung durch die Eltern ist immer auch zu prüfen, ob Mitmachaktionen u. Ä. auch gänzlich ohne oder mit dem absoluten Minimum an personenbezogene Daten realisiert werden können. Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datenminimierung, Zweckbindung, Transparenz, Löschung, Datensicherheit usw. → **Datenschutz-‚Basics‘**).

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen
für die Praxis
- 13 – 16-Jährige
- Unter 13-Jährige
- Kinderfreundliche Datenschutzerklärung

ABSOLUTES MUSS: KINDERFREUNDLICHE DATENSCHUTZERKLÄRUNG

Wenn Minderjährige einsichtsfähig sind und damit selbst einwilligen können, ist es von entscheidender Bedeutung, dass sie verständlich und umfassend mit Informationen zur Datenverarbeitung und deren Folgen versorgt werden. Die Datenschutzerklärung muss leicht auffindbar und in einfacher Sprache verständlich gefasst sein. Die Einwilligungserklärung in die Datenverarbeitung muss ebenfalls so gestaltet sein, dass die Minderjährigen leicht erkennen, in was sie tatsächlich einwilligen.

Gleiches gilt für Angebote an Kinder bis 13 Jahre: Bei Kinderangeboten spielt die Transparenz eine große Rolle. Je klarer dem Kind und auch den Erziehungsberechtigten die Notwendigkeit der Datenverarbeitung auch auf ‚normalen' Telemedienangeboten ohne Datenabfrage verdeutlicht wird, umso größer wird die Akzeptanz. Ebenso sollte in den Datenschutzhinweisen erklärt werden, wie lange die Daten für den Zweck vorgehalten werden, dass sie abschließend gelöscht werden, usw.

KEINE EINWILLIGUNG DER ELTERN 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. Das Konzept des Angebotes sollte daher auf seine medienpädagogische Relevanz geprüft werden:
Dient es auch der Prävention oder Beratung der Kinder/Jugendlichen?

ABSTIMMUNG MIT DER/DEM DATENSCHUTZBEAUFTRAGTEN

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

AUFTRAGSVERARBEITUNG

THEMEN

→ **Was sagt der Datenschutz**
- Auftragsverarbeitung
- Personenbezogene Daten
- Auftragsverarbeiter
- Datenübermittlung
- Auftragsverarbeitungs-vertrag
→ Empfehlungen für die Praxis

Vergibt die Rundfunkanstalt Aufträge an Dritte – z. B. für Hosting, Medienforschung usw. – und verarbeitet der externe Dienstleister dabei personenbezogene Daten im Auftrag der Rundfunkanstalt – z. B. der Nutzenden – müssen gesetzliche und hausinterne Regelungen zur Auftragsverarbeitung beachtet werden. In diesem Kontext gewinnen Cloud-Dienste an Bedeutung.

WAS SAGT DER DATENSCHUTZ?

AUFTRAGSVERARBEITUNG

Auftragsverarbeitung liegt vor, wenn die Rundfunkanstalt einen Dienstleister mit der Verarbeitung personenbezogener Daten nach seinen Weisungen betraut (z. B. Newsletter-Verwaltung, IT-Dienstleistungen mit Fernzugriff auf personenbezogene Daten der Rundfunkanstalt, externe Rechenzentren, E-Mail-Provider, Cloud-Anbieter, externe Agenturen zur Durchführung von Marketingevents). Auftragsverarbeiter handeln auf Weisung und im Interesse der Rundfunkanstalt, auch wenn es gewisse eigene Entscheidungsspielräume für sie geben kann.

Eine Beauftragung, bei der nicht die Datenverarbeitung personenbezogener Daten im Vordergrund steht bzw. bei der die Datenverarbeitung personenbezogener Daten nicht zumindest einen wichtigen (Kern-)Bestandteil ausmacht, stellt keine Auftragsverarbeitung im datenschutzrechtlichen Sinne dar.

Keine Auftragsvereinbarung besteht mangels Weisungsgebundenheit in der Inanspruchnahme fremder Fachleistungen bei einem **eigenständig Verantwortlichen** (z. B. Telekommunikations-Dienstleistungen).

Legen die Rundfunkanstalten mit einem Vertragspartner gemeinsam Zwecke und Mittel der Verarbeitung fest, so sind sie sog. **gemeinsam Verantwortliche**. In diesem Fall ist in einer Vereinbarung gemäß Artikel 26 DSGVO festzulegen, wer welchen datenschutzrechtlichen Pflichten gegenüber Betroffenen nachkommt (z. B. Information oder Auskunft).

THEMEN

→ Was sagt der Datenschutz
- Auftragsverarbeitung
- Personenbezogene Daten
- Auftragsverarbeiter
- Datenübermittlung
- Auftragsverarbeitungs-vertrag
→ Empfehlungen für die Praxis

PERSONENBEZOGENE DATEN

Bei der Nutzung von Telemedienangeboten werden in der Regel folgende Kategorien personenbezogener Daten durch die Auftragsverarbeiter verarbeitet: **Inhaltsdaten, Nutzerdaten** (z. B. zur Anmeldung oder Personalisierung) oder **Log-Informationen**, die der Nachverfolgung von Änderungen der Daten und am System dienen.

GEEIGNETE AUFTRAGSVERARBEITER

Wenn ein Dritter für die Durchführung einer eigenen Datenverarbeitungsaufgabe der Rundfunkanstalt ausgewählt wird (Auftragsverarbeiter), bleibt die **Rundfunkanstalt** gegenüber den Nutzer:innen **datenschutzrechtlich verantwortlich**. Deshalb hat die Rundfunkanstalt bei der Auswahl von Dienstleistern sorgfältig zu prüfen, ob der Anbieter geeignet ist und die **Eignung** der **technischen und organisatorischen Maßnahmen** (TOM) fortlaufend zu **kontrollieren**.

Für die Beurteilung der TOM ist der vorher durch den Fachbereich festgelegte Schutzbedarf der verarbeiteten Daten heranzuziehen. Auf Basis des Schutzbedarfs ist vom Dienstleister ein IT-Sicherheitskonzept zu erstellen, das Maßnahmen zusichert, die von der Rundfunkanstalt auf Geeignetheit zu prüfen sind. Die Maßnahmen können sich zum Beispiel auf die Übertragungswege der Daten zum und vom Dienstleister sowie auf die Gegebenheiten beim Dienstleister vor Ort beziehen.

DATENÜBERMITTLUNG AN EIN DRITTLAND

Verlassen die im Auftrag verarbeiteten personenbezogenen Daten den **Europäischen Wirtschaftsraum** (EWR) und gibt es für das Drittland keinen **Angemessenheitsbeschluss** der EU-Kommission, muss ein mit der EU vergleichbares Datenschutzniveau durch sog. „geeignete Garantien" (Art. 46 DSGVO) sichergestellt werden (→ **Datenschutz-‚Basics'**).

AUFTRAGSVERARBEITUNGSVERTRAG

Der Abschluss eines Auftragsverarbeitungsvertrages ist gesetzlich vorgeschrieben und regelt die Rechte und Pflichten zwischen Auftraggebern und weisungsgebundenen Auftragsverarbeitern (sowie ggf. von diesen eingesetzten sog. Unterauftragnehmern).

Ein Muster-Auftragsverarbeitungsvertrag wurde im AK DSB erarbeitet und den Rundfunkanstalten (auch in englischer Sprache) zur Verfügung gestellt.

THEMEN

→ Was sagt der Datenschutz
- Auftragsverarbeitung
- Personenbezogene Daten
- Auftragsverarbeiter
- Datenübermittlung
- Auftragsverarbeitungsvertrag

→ **Empfehlungen für die Praxis**

EMPFEHLUNGEN FÜR DIE PRAXIS

> prüfen, ob personenbezogene Daten der Rundfunkanstalt im Auftrag verarbeitet werden; wenn ja, Schutzbedarf erheben;

> Geeignetheit der vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen anhand des Schutzbedarfs prüfen;

> ermitteln, ob die im Auftrag verarbeiteten personenbezogenen Daten den EWR verlassen;

> Auftragsverarbeitungsvertrag (ggfs. → **Standardvertragsklauseln**) abschließen, der die vorgenannten Punkte rechtsverbindlich dokumentiert;

> über den Einsatz von Auftragsverarbeitern bzw. Drittstaatenübermittlung informieren (→ **Datenschutzerklärung**).

CHATS, FOREN, GÄSTEBÜCHER, KOMMENTARFUNKTION

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Regelmäßig u. zwangsläufig erhobene Daten
- Löschung von persönlichen Nutzerdaten – Löschung von Inhalten
- Nutzungsbedingungen und Netiquette
- Datensicherheit

Chats, Kommentarfunktionen und andere interaktive Tools zur Kommunikation mit den Nutzer:innen und zum Austausch der Nutzer:innen untereinander, einschließlich der Veröffentlichung eigener Inhalte wie z. B. Fotos oder Videos (sog. User Generated Content), sind fester Bestandteil öffentlich-rechtlicher Online-Angebote. Um sicherzustellen, dass diese Tools datenschutzkonform eingesetzt werden und der Austausch konstruktiv bleibt, bedarf es klarer Regelungen und redaktioneller Begleitung.

WAS SAGT DER DATENSCHUTZ?

Wer auf einer Website Chats, Foren etc. anbietet, verarbeitet personenbezogene Daten und Inhalte der Nutzer:innen. In den meisten Fällen müssen die Nutzer:innen eine E-Mail-Adresse angeben und sich unter Umständen auch mit weiteren Daten registrieren. Ob eine Registrierung erfolgen soll, ist eine redaktionelle Entscheidung. Datenschutzrechtlich ist zu beachten, dass bereits aufgrund der Übermittlung der IP-Adresse und erst recht durch die Angabe einer E-Mail-Adresse und eines etwaigen zusätzlichen Benutzernamens ein Personenbezug entsteht. Auch der Inhalt eines (vermeintlich) anonymen Beitrags kann also einen Personenbezug im rechtlichen Sinne aufweisen. Auch kann der Inhalt das Recht Dritter auf informationelle Selbstbestimmung verletzen. Das kann z. B. der Fall sein, wenn personenbezogene Daten wie Anschriften, E-Mail-Adressen oder Telefonnummern Dritter in Kommentaren veröffentlicht werden. Gleiches gilt für private Korrespondenz wie z. B. Briefe und E-Mails. Kommentare, Chats und interaktive Foren sind daher laufend (redaktionell) zu begleiten und zu prüfen.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Regelmäßig u. zwangsläufig erhobene Daten**
- **Löschung von persönlichen Nutzerdaten – Löschung von Inhalten**
- Nutzungsbedingungen und Netiquette
- Datensicherheit

EMPFEHLUNGEN FÜR DIE PRAXIS

REGELMÄSSIG UND ZWANGSLÄUFIG ERHOBENE DATEN

In der Regel fallen folgende personenbezogene Daten an:

> E-Mail-Adressen
> Nutzernamen
> die Beiträge der Nutzer:innen
> Log-In-Daten

Für die Teilnahme an Chats, Foren usw. sind diese Daten regelmäßig erforderlich. Mit der Teilnahme bzw. Registrierung erteilen die Nutzer:innen der Rundfunkanstalt konkludent die Einwilligung, diese personenbezogenen Daten zu verarbeiten.

Bei einer Registrierung für Chats oder den Beitritt zu einem Forum gilt, dass nur so viele personenbezogene Daten der Nutzer:innen wie unbedingt nötig abfragt und diese Daten nur für den konkreten Zweck (Zugang zum Forum usw.) gespeichert und genutzt werden dürfen. Eine Double-Opt-In-Lösung ist empfehlenswert. Im Falle einer Registrierung sollte die zuständige Redaktion zudem vorsehen, dass die Nutzer:innen einen Nickname wählen können, damit so auf die Veröffentlichung des Klarnamens verzichtet werden kann. Es ist nützlich, im Rahmen der Registrierung die wichtigsten Informationen für die Nutzer:innen kompakt zusammenzufassen. Die Details können dann mit einem weiteren Klick – z. B. in der allgemeinen Datenschutzerklärung – verfügbar gemacht werden. Auch auf die → **Nutzungsbedingungen/Netiquette** sollte verlinkt werden.

Eine aktive Einholung von Einwilligungen der Nutzer:innen für die Veröffentlichung ihrer Beiträge in Chats etc. ist nicht erforderlich. Denn die Inhalte der Nutzer:innen werden Bestandteil des journalistisch-redaktionellen Angebots der Rundfunkanstalt und unterliegen dem → **Medienprivileg**.

LÖSCHUNG VON PERSÖNLICHEN NUTZERDATEN – LÖSCHUNG VON INHALTEN

Die Nutzer:innen müssen die Möglichkeit haben, sich jederzeit abmelden und ihre Daten löschen (lassen) zu können. Im Falle einer Abmeldung muss der Account unverzüglich gelöscht werden. Es empfiehlt sich, den Nutzer:innen die Möglichkeit einzuräumen, ihre Accounts selbst zu löschen (die Kommentare können dann z. B. neutral ‚Gast' zugewiesen werden).

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Regelmäßig u. zwangsläufig erhobene Daten
- Löschung von persönlichen Nutzerdaten – Löschung von Inhalten
- **Nutzungsbedingungen und Netiquette**
- **Datensicherheit**

NUTZUNGSBEDINGUNGEN UND NETIQUETTE

Die Rundfunkanstalten haben in Nutzungsbedingungen bzw. in einer Netiquette die Rahmenbedingungen festzulegen, die von Nutzer:innen vor ihrer Teilnahme an Chats, Foren usw. akzeptiert werden müssen. Darin ist u. a. definiert, welche Form der Kommunikation erwünscht ist, was verboten ist und wie bei Verstößen vorgegangen wird. Anders als die → **Datenschutzerklärung**, der nicht zugestimmt werden kann und muss, sollten die Nutzungsbedingungen bzw. die Netiquette aktiv bestätigt werden (z. B. via Checkbox).

Wenn die Inhalte der Nutzer:innen nicht den Vorgaben der Nutzungsbedingungen bzw. der Netiquette entsprechen, können sie gelöscht und die Nutzer:innen im Extremfall für eine gewisse Zeit gesperrt werden. Dies sollte so in den Nutzungsbedingungen bzw. der Netiquette erläutert werden und ist u. a. dann von Bedeutung, wenn Dritte durch die Veröffentlichung in ihrem Recht auf informationelle Selbstbestimmung verletzt sind. Unter welchen Voraussetzungen und nach welchem Verfahren Sperrungen von Nutzer:innen erfolgen können, ist eine medienrechtliche Fragestellung und ggfs. mit den Justiziariaten abzustimmen.

AUF DATENSICHERHEIT ACHTEN

Aus dem Prinzip der Datensicherheit folgt, dass geeignete Sicherheitsmaßnahmen, insbesondere etwa für die personenbezogenen Daten wie die übermittelten E-Mail-Adressen, ergriffen werden müssen.

KONTAKTFORMULARE, NEWSLETTER

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Zweckbindung, Datensparsamkeit und Einwilligung
- Besonderheiten beim Newsletter
- Datenschutzerklärung
- Datensicherheit
- Minderjährigen-Datenschutz
- Externe Dienstleister

Das Internet bietet für die Rundfunkanstalten vielfältige Möglichkeiten der Kontaktaufnahme mit den Nutzer:innen ihrer Angebote. Häufig werden dafür Online-Kontaktformulare eingesetzt. Über Newsletter kann gezielt über ausgewählte Themen informiert werden.

WAS SAGT DER DATENSCHUTZ?

Auch beim Kontakt mit den Nutzer:innen gilt Folgendes: Es sollen als Pflichtangaben immer nur so viele personenbezogene Daten wie unbedingt nötig abfragt werden. Die abgefragten Daten dürfen immer nur für einen bestimmten, genau benannten Zweck genutzt und nur so lange gespeichert werden, wie es tatsächlich erforderlich ist. Danach ist eine Löschung oder Anonymisierung erforderlich.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Zweckbindung, Datensparsamkeit und Einwilligung**
- **Besonderheiten beim Newsletter**
- Datenschutzerklärung
- Datensicherheit
- Minderjährigen-Datenschutz
- Externe Dienstleister

EMPFEHLUNGEN FÜR DIE PRAXIS

ZWECKBINDUNG, DATENSPARSAMKEIT UND EINWILLIGUNG

Die Rundfunkanstalt darf nur solche Daten als Pflichtangaben abfragen, die für den konkreten Zweck – Kontaktaufnahme, Zusendung eines Newsletters usw. – unbedingt notwendig sind (kein ‚nice to have', sondern ‚must have'; → **Datenschutz-‚Basics'**). Die Pflichtfelder sind entsprechend kenntlich zu machen.

Sofern in einem Kontaktformular weitere personenbezogene Daten abgefragt werden, ist darauf hinzuweisen, dass dies keine Pflichtangaben, sondern freiwillige Angaben sind. Die Nutzer:innen müssen auch hinsichtlich der freiwilligen Angaben wissen, für welche Zwecke sie ihre Daten an die Rundfunkanstalt übermitteln und auf dieser Basis eine informierte Einwilligung (→ **Datenschutz-‚Basics'**) erteilen. Auch über eine etwaige Weitergabe ihrer Daten müssen die Nutzer:innen vorab informiert werden. Auf die Möglichkeit des jederzeitigen Widerrufs der Einwilligung ist hinzuweisen.

Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es erforderlich ist und für keine anderen Zwecke verwendet werden.

BESONDERHEITEN BEIM NEWSLETTER

Die Nutzer:innen müssen Newsletter ausdrücklich bestellen, d. h.: Newsletter dürfen nie unverlangt zugesandt werden.

> Zur rechtssicheren Erklärung der Einwilligung ist das ‚Double-Opt-In'-Verfahren einzusetzen: Die Interessent:innen erhalten nach der Anmeldung eine Begrüßungsnachricht, in der aufgefordert wird, einen Link anzuklicken. Erst danach darf die E-Mail-Adresse für den Empfang des Newsletters aktiviert werden. Damit kann verhindert werden, dass jemand eine fremde E-Mail-Adresse verwendet. Der gesamte Vorgang ist zu dokumentieren, weil die erteilte Einwilligung der Nutzer:innen ggf. auf Nachfrage nachzuweisen ist.

> In jedem Newsletter müssen die Nutzer:innen deutlich sichtbar darauf hingewiesen werden, dass die Newsletter jederzeit abbestellt werden können. Hierzu ist ein Kontakt-Link in die Newsletter-E-Mail zu setzen.

> Wie immer gilt die Zweckbindung: Daten der Nutzer:innen, die der Rundfunkanstalt z. B. im Rahmen der Bestellung eines Newsletters übermittelt wurden, dürfen auch nur für diesen Newsletter und nur so lange genutzt werden, wie das Abo läuft. Sobald die Nutzer:innen den Newsletter abbestellen, sind ihre Daten zu löschen bzw. zu anonymisieren.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Zweckbindung, Datensparsamkeit und Einwilligung
- Besonderheiten beim Newsletter
- **Datenschutzerklärung**
- **Datensicherheit**
- **Minderjährigen-Datenschutz**
- **Externe Dienstleister**

INFORMATIONEN IN DER DATENSCHUTZERKLÄRUNG

In der allgemeinen Datenschutzerklärung sind die Nutzer:innen über die Möglichkeiten der Kontaktaufnahme zu informieren. Diese Information ersetzt jedoch nicht die notwendige Einwilligung im jeweiligen Einzelfall einer Kontaktaufnahme.

AN DIE LÖSCHUNG DENKEN

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Maßgeblich ist der Inhalt der übermittelten Informationen und der Zweck der Datenverarbeitung (journalistisch-redaktionelle Nutzung der Daten, Teilnehmerdaten aufgrund von Programmaktionen oder Gewinnspielen etc.).

Es ist sinnvoll, sich generell auf ein Löschkonzept zu verständigen. Außerdem muss sichergestellt werden, dass nach der Speicherfrist auch tatsächlich eine Löschung oder Anonymisierung der Daten erfolgt.

DATENSICHERHEIT – VERSCHLÜSSELTE ÜBERTRAGUNG

Die Kommunikation mit Nutzer:innen über das Internet ist so sicher wie möglich zu gestalten, sobald personenbezogene Daten übertragen werden (was regelmäßig der Fall ist). 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 (dies gilt auch für den E-Mail-Kontakt). Die IT-Sicherheitsbeauftragten der Rundfunkanstalten können diesbezüglich beraten.

MINDERJÄHRIGEN-DATENSCHUTZ

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

EINSATZ VON EXTERNEN DIENSTLEISTERN

Wird ein externer Dienstleister für den konkreten Kontakt mit den Nutzer:innen mit der Durchführung und/oder dem Hosting der Nutzerdaten beauftragt ist, sind die Hinweise zur → **Auftragsverarbeitung** zu beachten.

GEWINNSPIELE

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Teilnahmebedingungen
- Zweckbindung und Datensparsamkeit
- An die Löschung denken
- Minderjährigen-Datenschutz
- Externe Dienstleister
- Beachtung sonstiger Vorgaben
- Drittplattformen

Gewinnspiele werden als Teil des redaktionellen Angebots auch in den Telemedienangeboten der Rundfunkanstalten veranstaltet. Es gibt Gewinnspiele in den eigenen Telemedienangeboten der Rundfunkanstalten und in den Angeboten der Rundfunkanstalten auf Drittplattformen.

WAS SAGT DER DATENSCHUTZ?

Welche Nutzerdaten 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 darauf zu achten, dass verpflichtend nur die Daten erhoben werden, die für die Durchführung des Gewinnspiels tatsächlich notwendig sind. Rechtsgrundlage für die Verarbeitung der Nutzerdaten ist der Gewinnspielvertrag (Art. 6 Abs. 1 S. 1 lit. b DSGVO). Die erhobenen Daten dürfen nur zur Durchführung des Gewinnspiels verwendet werden. Sie dürfen auch nur so lange gespeichert werden, wie es für die Durchführung und Abwicklung des Gewinnspiels erforderlich ist. Danach sind die Daten zu löschen. In der → **Datenschutzerklärung** für das Gewinnspiel muss über Art und Umfang der Datenverarbeitung unter Nennung der einschlägigen Rechtsgrundlage und über die Betroffenenrechte informiert werden.

Für jede über die Teilnahme am Gewinnspiel hinausgehende Nutzung von Teilnehmerdaten (z. B. für die Zusendung eines Newsletters bzw. für die freiwillige Angabe weiterer personenbezogener Daten) ist eine ausdrückliche Einwilligung einzuholen. Dabei muss deutlich gemacht werden, dass die Erteilung der Erlaubnis zur Nutzung der Daten für andere Zwecke freiwillig ist und keine Auswirkung auf das Gewinnspiel hat.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Teilnahmebedingungen**
- **Zweckbindung und Datensparsamkeit**
- An die Löschung denken
- Minderjährigen-Datenschutz
- Externe Dienstleister
- Beachtung sonstiger Vorgaben
- Drittplattformen

EMPFEHLUNGEN FÜR DIE PRAXIS

TEILNAHMEBEDINGUNGEN MIT INFORMATIONEN ZUM DATENSCHUTZ

Die spezifische Datenschutzerklärung für das Gewinnspiel sollte zusammen mit den Teilnahmebedingungen unmittelbar auf der hierfür eingerichteten Seite oder über einen unmissverständlichen Link (‚Teilnahmebedingungen und Datenschutzhinweise') erreichbar sein. Ein Verweis auf die allgemeinen Datenschutzhinweise der Rundfunkanstalt dürfte i. d. R. nicht ausreichend sein.

ZWECKBINDUNG UND DATENSPARSAMKEIT

Die Rundfunkanstalt darf nur die Daten als Pflichtfelder abfragen, die für die Durchführung des Gewinnspiels erforderlich sind. Beispiele:

> Die Abfrage der Mailadresse ist ausreichend, wenn ein Versand des Preises (z. B. Tickets) online erfolgt oder um eine Identifikation zu ermöglichen (z. B. um eine Mehrfachteilnahme zu verhindern).
> Die (zusätzliche) Abfrage der 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. In der Regel ist hier jedoch eine vorherige Kontaktaufnahme per E-Mail oder Telefon mit den Gewinner:innen möglich, so dass eine Adressangabe als Pflichtfeld nicht immer erforderlich ist.

Alle weiteren personenbezogenen Daten dürfen nur als freiwillige Angaben abgefragt werden, immer verbunden mit dem ausführlichen Datenschutzhinweis, zu welchem Zweck die konkrete Datenverarbeitung erfolgt und dass die Daten nicht an Dritte weitergegeben werden.
Die Nutzer:innen sind darüber zu informieren, dass sie für die weiteren freiwilligen Angaben ihre Einwilligung in die Datenverarbeitung jederzeit widerrufen können.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Teilnahmebedingungen
- Zweckbindung und Datensparsamkeit
- **An die Löschung denken**
- **Minderjährigen-Datenschutz**
- **Externe Dienstleister**
- **Beachtung sonstiger Vorgaben**
- **Drittplattformen**

AN DIE LÖSCHUNG DENKEN

Die im Zusammenhang mit dem Gewinnspiel erhobenen Daten der Teilnehmer:innen sind zu löschen, sobald das Gewinnspiel beendet und eine angemessene Reklamationszeit abgelaufen ist. Bitte beachten: Die Daten der Gewinner:innen sind möglicherweise auch nach Beendigung des Gewinnspiels an anderen Stellen innerhalb der Rundfunkanstalt zu Dokumentationszwecken für eine gewisse Zeit zu archivieren (bitte hausintern, z. B. mit Finanzen oder Revision, klären). Sofern keine entsprechende Programmierung erfolgen kann, muss notfalls eine manuelle Löschung vorgenommen werden. Ausnahme: Personenbezogene Daten, die im Rahmen des Gewinnspiels zu redaktionellen Zwecken genutzt werden, z. B. eingesandte Fotos und Geschichten, können aufgrund des → **Medienprivilegs** auch langfristig gespeichert werden. Es gelten die gesetzlichen Aufzeichnungspflichten für Rundfunksendungen.

MINDERJÄHRIGEN-DATENSCHUTZ

Beim Umgang mit Daten von Minderjährigen gelten die Hinweise zum → **Minderjährigen-Datenschutz** .

EINSATZ VON EXTERNEN DIENSTLEISTERN

Sofern ein Dienstleister mit der Durchführung und/oder dem Hosting für das Gewinnspiel beauftragt ist, sind die Hinweise zur → **Auftragsverarbeitung** zu beachten.

BEACHTUNG DER SONSTIGEN VORGABEN FÜR GEWINNSPIELE

Zusätzlich relevant sind die sonstigen Vorgaben der öffentlich-rechtlichen Rundfunkanstalten für Gewinnspiele (vgl. die sendereigenen Richtlinien für Werbung, Sponsoring, Gewinnspiele und Produktionshilfe).

DRITTPLATTFORMEN

Bei Gewinnspielen auf → **Drittplattformen** sind auch die vertraglichen Vorgaben der Betreiber maßgeblich, die die Veranstaltung von Gewinnspielen einschränken können.

VOTINGS

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Zweckbindung und Datensparsamkeit
- Datenschutzerklärung
- Absicherung gegen Manipulation
- An die Löschung denken
- Einsatz von Dienstleistern
- Verknüpfung mit Gewinnspiel
- Verschlüsselung
- Minderjährigen-Datenschutz

Votings (Abstimmungen) sind für viele Redaktionen ein attraktives Element der Programmgestaltung. Durch den direkten Rückkanal sollen die Nutzer:innen am Programm und dessen Gestaltung 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 einschließlich Mitmachmöglichkeiten im eigenen Telemedien-Angebot der Rundfunkanstalten und auf Drittplattformen.

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:innen hierüber ausreichend zu informieren. Es sind so wenig 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. Nach Abschluss des Votings ist eine Löschung erforderlich.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Zweckbindung und Datensparsamkeit**
- **Datenschutzerklärung**
- **Absicherung gegen Manipulation**
- **An die Löschung denken**
- Einsatz von Dienstleistern
- Verknüpfung mit Gewinnspiel
- Verschlüsselung
- Minderjährigen-Datenschutz

EMPFEHLUNGEN FÜR DIE PRAXIS

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 nicht für andere Zwecke verwendet werden.

INFORMATIONEN IN DER DATENSCHUTZERKLÄRUNG

Vorab sind Ablauf und Bedingungen für das Voting festzulegen und hierüber in der Datenschutzerklärung zu informieren.

ABSICHERUNG GEGEN MANIPULATION

Bei internetbasierten Abstimmungsformen können aus redaktionellen Gründen unter Berücksichtigung der Nutzerfreundlichkeit technische Absicherungen gegen Manipulation von außen zum Einsatz kommen (z. B. Sperrung der IP-Adresse für ein bestimmtes Zeitfenster, Programme zur Identifizierung von Robotern, Identifizierung per E-Mail, Cookies). Auch in diesem Fall dürfen nur solche Daten der Nutzer:innen verarbeitet und mitgeloggt werden, die für die korrekte Durchführung des Votings erforderlich sind. Zudem ist ein entsprechender Hinweis in der Datenschutzerklärung erforderlich.

AN DIE LÖSCHUNG DENKEN

Es sind Löschfristen festzulegen und darauf zu achten, dass die Daten gelöscht werden, sobald eine angemessene Reklamationszeit nach Beendigung des Votings abgelaufen ist. Falls keine automatische Löschung eingerichtet werden kann, müssen die Daten notfalls manuell gelöscht werden.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Zweckbindung und Datensparsamkeit
- Datenschutzerklärung
- Absicherung gegen Manipulation
- An die Löschung denken
- **Einsatz von Dienstleistern**
- **Verknüpfung mit Gewinnspiel**
- **Verschlüsselung**
- **Minderjährigen-Datenschutz**

EINSATZ VON DIENSTLEISTERN

Sofern ein externer Dienstleister mit der Durchführung und/oder dem Hosting eines Votings beauftragt ist, gelten die Hinweise zur → **Auftragsverarbeitung**.

VERKNÜPFUNG MIT GEWINNSPIEL

Eine Teilnahme am Voting kann mit einem Gewinnspiel kombiniert werden (z. B.: „Unter den ‚Voter:innen' werden Tickets verlost."). In diesem Fall sind zusätzlich die Hinweise zu Gewinnspielen zu beachten.

VERSCHLÜSSELUNG

Die Kommunikation mit Nutzer:innen 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 siehe auch die Hinweise zum → **Minderjährigen-Datenschutz**.

APPS

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Personenbeziehbare Daten
- Datenschutzfreundliche App-Entwicklung
- Grundsatz der Zweckbindung
- Grundsätze beim Einsatz von Identifiern/Cookies
- Verarbeiten von personenbezogenen Daten
- Nutzungsmessung
- Push-Funktionen
- Standortdaten
- Inhalte von Drittanbietern
- Datenschutzerklärung
- Datensicherheit
- Beauftragung von Dritten
- Minderjährigen-Datenschutz

Unter Apps versteht man Anwendungssoftware für digitale Endgeräte, wobei es sehr unterschiedliche Formen gibt. Die Rundfunkanstalten nutzen Apps, um ihre journalistischen Angebote darüber zu verbreiten.
Apps werden regelmäßig über App-Stores der verschiedenen Betriebssystem-Anbieter (Apple, Google etc.) angeboten. Dadurch entstehen komplexe rechtliche Beziehungen zwischen App-Store-Betreiber, App-Anbieter und Nutzer:innen, die insbesondere für Letztere nicht leicht nachzuvollziehen sind.

WAS SAGT DER DATENSCHUTZ?

Beim Herunterladen von Apps aus einem App-Store, aber auch bei der Nutzung von Apps werden personenbezogene Daten der Nutzer:innen verarbeitet. Hier ist zu beachten, dass dabei in der Regel sowohl beim Store-Betreiber als auch beim Anbieter der App Daten verarbeitet werden.

Bei der Nutzung einer App werden, je nach Typ, Funktionalität und Gestaltung verschiedene personenbezogene Daten der Nutzer:innen verarbeitet. Dabei kann es sich um Bankdaten, um Zugriffe auf gespeicherte Fotos/Adressbücher, Standortdaten usw. handeln. Die größten Datenschutzrisiken liegen für Nutzer:innen insofern in der mangelnden Kenntnis der von einer App auf der jeweiligen Plattform ausgeführten Verarbeitung ihrer Daten.

Die Rundfunkanstalt ist datenschutzrechtlich für die bei der Ausführung der von ihr angebotenen App anfallenden Nutzerdaten vollumfänglich verantwortlich. Dies gilt auch dann, wenn die App über den Server eines Dienstleisters betrieben wird. Die Rundfunkanstalt muss auch bei den Entwicklungsanweisungen des App-Store-Betreibers oder Drittanbieters (z. B. für die Nutzungsmessung) genau prüfen, inwieweit der in die App einzubauende Code zu einer Verarbeitung von Nutzerdaten führt.

Wichtig ist der Hinweis auf eine Datenschutzerklärung, die vor dem Herunterladen der App eingesehen werden kann und die auf die Besonderheiten der Datenverarbeitung bei der App-Nutzung hinweist. Bei der Gestaltung und Ausführung der App sind die allgemeinen Anforderungen der DSGVO zu beachten.

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Personenbeziehbare Daten
- Datenschutzfreundliche App-Entwicklung
- Grundsatz der Zweckbindung
- Grundsätze beim Einsatz von Identifiern/Cookies
- Verarbeiten von personenbezogenen Daten
- Nutzungsmessung
- Push-Funktionen
- Standortdaten
- Inhalte von Drittanbietern
- Datenschutzerklärung
- Datensicherheit
- Beauftragung von Dritten
- Minderjährigen-Datenschutz

Dies betrifft insbesondere den Grundsatz der Datensparsamkeit (Privacy by Design) und die IT-Sicherheit (→ **Datenschutz-‚Basics'**).

Die Verantwortung für die Verarbeitung von Nutzerdaten bei der Anmeldung zum Store und beim Aufrufen der App zum Herunterladen liegt in der Regel beim App-Store-Betreiber. Beim Versenden von Push-Nachrichten kommt es auf die Gestaltung an (→ **Empfehlungen für die Praxis**). Der Umfang der Datenverarbeitung und die Aufklärung der Nutzer:innen darüber ist bei einigen Plattformen/Store-Betreibern datenschutzrechtlich nicht immer unbedenklich. Auch wenn die Datenverarbeitung für den Betrieb des App-Stores bei dessen Betreiber liegt, so muss doch immer wieder hinterfragt werden, auf welchen Plattformen bzw. in welchen Stores die öffentlich-rechtlichen Rundfunkanstalten vertreten sein und wo man gegebenenfalls auf eine Präsenz verzichten sollte.

EMPFEHLUNGEN FÜR DIE PRAXIS

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Personenbeziehbare Daten**
- **Datenschutzfreundliche App-Entwicklung**
- Grundsatz der Zweckbindung
- Grundsätze beim Einsatz von Identifiern/Cookies
- Verarbeiten von personenbezogenen Daten
- Nutzungsmessung
- Push-Funktionen
- Standortdaten
- Inhalte von Drittanbietern
- Datenschutzerklärung
- Datensicherheit
- Beauftragung von Dritten
- Minderjährigen-Datenschutz

Als App-Anbieter und -Entwickler hat die Rundfunkanstalt auf Folgendes zu achten:

PERSONENBEZIEHBARE DATEN

Apps verarbeiten Informationen, die auf den ersten Blick nicht immer als personenbezogene Daten zu erkennen sind. Die Bestimmbarkeit der nutzenden Person im Zusammenhang mit mobilen Geräten und Apps ist nämlich nicht nur bei Namen, Adress-/Zahlungsdaten und Bildern/Videos etc., sondern u. a. auch anhand folgender Informationen möglich:

> IP-Adresse
> Standortdaten
> ggf. gewählte Bezeichnung des Telefons (Nutzer:innen neigen dazu, ihr Telefon unter Verwendung ihres eigenen Namens zu benennen, z. B. „Max Mustermanns iPhone“)
> ggf. Browserverlauf
> Authentifizierungsdaten für spezielle Dienste, insbesondere Social Media

DATENSCHUTZFREUNDLICHE APP-ENTWICKLUNG

Die Rundfunkanstalt sollte in der Entstehungs- und Entwicklungsphase einer App den datenschutzrechtlichen Vorgaben durch eine entsprechende technische Gestaltung (Privacy by Design) sowie datenschutzfreundliche Voreinstellungen (Privacy by Default) Rechnung 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. Die Nutzer:innen sollten die Möglichkeit haben, die wesentlichen Funktionalitäten der App ohne weitere personenbezogene Angaben (Klarname, Standort) zu nutzen.

Auch bei den Installationsanweisungen der App-Store-Betreiber ist zu prüfen, ob für die Funktionalität bzw. Einstellung der App in den Store alle vom Store-Betreiber angegebenen Codes/Identifier erforderlich sind. Dies ist u. a. bei Werbe-IDs für die Angebote der öffentlich-rechtlichen Rundfunkanstalten in der Regel nicht der Fall.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Personenbeziehbare Daten
- Datenschutzfreundliche App-Entwicklung
- **Grundsatz der Zweckbindung**
- **Grundsätze beim Einsatz von Identifiern/Cookies**
- **Verarbeiten von personenbezogenen Daten**
- Nutzungsmessung
- Push-Funktionen
- Standortdaten
- Inhalte von Drittanbietern
- Datenschutzerklärung
- Datensicherheit
- Beauftragung von Dritten
- Minderjährigen-Datenschutz

BERECHTIGUNGEN NUR NACH DEM GRUNDSATZ DER ZWECKBINDUNG ANFRAGEN

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

Hier gilt: Es dürfen nur die für die App tatsächlich erforderlichen Berechtigungen von Nutzer:innen angefordert werden. Bsp.: Nicht jede App benötigt für ihre Funktionalität einen Zugriff auf Kamera, Standort oder Adressbuch eines Endgerätes. Entsprechende Daten sollten in diesem Fall nicht abgefragt werden. Einige Betriebssysteme von mobilen Endgeräten bieten Berechtigungen nur in festen Kombinationen an, welche neben der erforderlichen Berechtigung auch nicht benötigte Berechtigungen enthalten. Die Rundfunkanstalt muss in einer für die App spezifischen Datenschutzerklärung über diesen Umstand aufklären und sich gegenüber den jeweiligen Nutzer:innen dazu verpflichten, von der nicht erforderlichen Berechtigung keinen Gebrauch zu machen.

ALLGEMEINE GRUNDSÄTZE BEIM EINSATZ VON IDENTIFIERN/COOKIES & CO. BEACHTEN

Es gilt der Grundsatz, dass für den Zugriff auf gespeicherte Informationen im Endgerät der Nutzer:innen eine Einwilligung erforderlich ist, es sei denn, der Zugriff ist unbedingt erforderlich, um die App zur Verfügung stellen zu können (→ **Cookies, Local-Storage-Elemente & Co.**).

ALLGEMEINE GRUNDSÄTZE BEIM VERARBEITEN VON PERSONENBEZOGENEN DATEN BEACHTEN

Werden bei der Nutzung der App weitere personenbezogene Daten (z. B. über entsprechende Formulare in der App) erhoben, so müssen dafür die Rechtsgrundlagen geprüft und im Falle der Einwilligung die allgemeinen Hinweise zur Einholung von Einwilligungen beachtet werden (→ **Datenschutz-‚Basics'**).

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Personenbeziehbare Daten
- Datenschutzfreundliche App-Entwicklung
- Grundsatz der Zweckbindung
- Grundsätze beim Einsatz von Identifiern/Cookies
- Verarbeiten von personenbezogenen Daten
- **Nutzungsmessung**
- **Push-Funktionen**
- Standortdaten
- Inhalte von Drittanbietern
- Datenschutzerklärung
- Datensicherheit
- Beauftragung von Dritten
- Minderjährigen-Datenschutz

GRUNDSÄTZE DER NUTZUNGSMESSUNG BEACHTEN

Auch bei Apps finden in der Regel statistische Nutzungsmessungen statt. In Bezug auf die Prüfung der Rechtsgrundlagen für die Datenverarbeitung bei Nutzungsmessungen wird auf → **Nutzungsmessung/Tracking** verwiesen. Greifen für Zwecke der Nutzungsmessung Identifier/Local-Storage-Elemente auf das Endgerät der Nutzer:innen zu, so gelten hierfür die allgemeinen Grundsätze zu → **Cookies, Local-Storage-Elemente & Co.** Auf die Nutzungsmessung ist in der Datenschutzerklärung der App entsprechend hinzuweisen.

PUSH-FUNKTIONEN RICHTIG EINRICHTEN

Mit der Push-Funktion können verschiedene Inhalte – z. B. Kurznachrichten, Live-Ticker usw. – von einem Server zu einem speziellen Mobilgerät versandt werden. Haben Nutzer:innen einmal den Dienst abonniert, übernimmt der Server eigeninitiativ das ‚Pushen' des Inhalts zu den Endgeräten.

Damit die Rundfunkanstalt weiß, wer welche Push-Nachrichten erhalten möchte, ist eine eindeutige Kennung erforderlich. Es wird empfohlen, hierfür keine persönlichen Angaben der Nutzer:innen, wie Name oder E-Mail-Adresse zu verwenden, sondern mit einer zufallsgenerierten eindeutigen Nummer (sog. Token oder Device-Token-ID) zu arbeiten: Mit Zustimmung der jeweiligen Nutzer:innen wird durch das Betriebssystem des Gerätes der Abonnent:innen 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 Nutzer:innen aber immerhin eingeschränkt, da die Token-ID außerhalb der App oder bei Neuinstallationen keinen Bezug mehr zu den jeweiligen Nutzer:innen ermöglicht.

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

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Personenbeziehbare Daten
- Datenschutzfreundliche App-Entwicklung
- Grundsatz der Zweckbindung
- Grundsätze beim Einsatz von Identifiern/Cookies
- Verarbeiten von personenbezogenen Daten
- Nutzungsmessung
- Push-Funktionen
- **Standortdaten**
- **Inhalte von Drittanbietern**
- **Datenschutzerklärung**
- Datensicherheit
- Beauftragung von Dritten
- Minderjährigen-Datenschutz

ACHTUNG BEI STANDORTDATEN

Sofern durch die App auf Standortdaten des Geräts zugegriffen wird, muss darauf geachtet werden, dass dies nur im zulässigen Umfang geschieht. Eine dauerhafte Speicherung von Standortdaten darf ohne gesonderte Einwilligung z. B. nur dann stattfinden, wenn dies für die Funktionalität des Dienstes unbedingt erforderlich ist. Meist ist es z. B. nicht unbedingt notwendig, dass der Standort der Nutzer:innen metergenau erhoben und verwendet wird. Darum empfiehlt sich eine gezielte ‚Verwaschung' des Standortes. Dies kann z. B. durch eine Nullung von Dezimalstellen in den GPS-Koordinaten vor Versand der Daten an den jeweiligen Dienste-Anbieter erreicht werden.

ACHTUNG BEIM EINBINDEN VON INHALTEN VON DRITTANBIETERN

Werden Inhalte von Drittanbietern in die App eingebunden, besteht die Möglichkeit, dass allein durch das Aktivieren der App Nutzerdaten ohne Wissen und Wollen der jeweiligen Nutzer:innen an die Drittanbieter fließen. Hier muss, genau wie bei einer Website, auf eine datenschutzkonforme Gestaltung geachtet werden (→ **Embedding von Fremdinhalten**).

APP-SPEZIFISCHE DATENSCHUTZERKLÄRUNG AUCH SCHON VOR DER INSTALLATION BEREITHALTEN

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 (s. hierzu auch die allgemeinen Hinweise unter → **Datenschutzerklärung**).

Eine einfache Verknüpfung mit der Datenschutzerklärung des Webangebotes der Rundfunkanstalt genügt in der Regel nicht, wenn dort die Besonderheiten der Datenverarbeitung in der App fehlen. Die Möglichkeit zur Kenntnisnahme der App-spezifischen Datenschutzerklärung muss auch schon vor der Installation der App gewährleistet sein. Die Datenschutzerklärung kann dafür im App-Store als Link zum Abruf bereitgehalten werden.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Personenbeziehbare Daten
- Datenschutzfreundliche App-Entwicklung
- Grundsatz der Zweckbindung
- Grundsätze beim Einsatz von Identifiern/Cookies
- Verarbeiten von personenbezogenen Daten
- Nutzungsmessung
- Push-Funktionen
- Standortdaten
- Inhalte von Drittanbietern
- Datenschutzerklärung
- **Datensicherheit**
- **Beauftragung von Dritten**
- **Minderjährigen-Datenschutz**

AUF DATENSICHERHEIT ACHTEN

Eine wichtige Rolle bei der datenschutzgerechten Gestaltung spielt die Sicherheit einer App. Dazu gehört z. B. das Thema Transportverschlüsselung in Bezug auf die Kommunikation zwischen Nutzer:in und Rundfunkanstalt. Auf die allgemeinen Hinweise zur Datensicherheit in → **Datenschutz-‚Basics'** wird verwiesen.

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, gehostet oder betrieben wird oder sonstige Daten (z. B. Device-Token-ID) durch einen externen Dienstleister verarbeitet werden. Hier gelten die Hinweise zur → **Auftragsverarbeitung**.

MINDERJÄHRIGEN-DATENSCHUTZ BEACHTEN

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

COOKIES, LOCAL-STORAGE-ELEMENTE & CO.

THEMEN

→ Was sagt der Datenschutz
- Zugriff auf das Endgerät
- Datenverarbeitung

→ Empfehlungen für die Praxis
- Regelmäßiger Check
- Drittanbieter-Cookies
- Einordnung
- Einwilligung
- Datenschutzerklärung

Bei Cookies und sog. Local-Storage-Elementen geht es ganz allgemein um Technologien, die im Endgerät von Nutzer:innen als Information abgelegt werden und auf die die Rundfunkanstalt bei Aufruf des Angebots zugreift.

Beim Betrieb von Websites werden in der Regel Cookies oder ähnliche Techniken wie Local-Storage-Elemente eingesetzt. Bei Cookies handelt es sich um kleine Textdateien, die lokal im temporären Speicher des Internet-Browsers der Nutzer:innen, also auf deren Endgerät (PC, Tablet, Handy etc.), gespeichert werden. Sie übermitteln von dort Daten an die Stelle, die die Cookies einsetzt. Das können rein technische Informationen, etwa zum Browser oder Endgerät, aber auch personenbezogene Daten wie die IP-Adresse sein.

Es gibt verschiedene Arten von Cookies, die zu unterschiedlichen Zwecken verwendet werden. So werden Cookies für den reibungslosen technischen Aufbau beim Betrieb von Websites eingesetzt. Darüber hinaus gibt es auch Cookies, die gesetzt werden, um die Nutzer:innen bzw. die Einstellungen (z. B. Sprache, Schriftgröße, Warenkorb), die sie gewählt haben, wiederzuerkennen und ihnen das Surfen auf einer Website funktional zu erleichtern. Der Einsatz bestimmter Cookies ermöglicht es aber auch, das Nutzungsverhalten, und zwar auch über mehrere Websites hinweg, zu ermitteln.
Cookies haben, je nach Zweck, eine sehr unterschiedliche Lebensdauer. Session-Cookies etwa werden automatisch gelöscht, wenn der/die Nutzer:in den Browser schließt. Cookies, in denen Einstellungen der jeweiligen Nutzer:innen (Sprache, Lautstärke beim Radioplayer, Schriftgröße) gespeichert werden, werden in der Regel als permanentes Cookie mit langer Laufzeit abgelegt.
Beim Aufruf einer Website können Cookies verschiedener Anbieter gesetzt werden. Neben den Cookies, die die Rundfunkanstalt als Betreiber der Website setzt, können auch Cookies von Dienstleistern im Zusammenhang mit der Nutzungsmessung oder Cookies von externen Anbietern, deren Inhalte auf der Website der Anstalt eingebettet sind, gesetzt werden (→ Embedding von Fremdinhalten).
Es gibt neben Cookies auch andere Technologien, die zu ähnlichen Zwecken eingesetzt werden und über die Informationen im Endgerät gespeichert werden. Solche Local-Storage-Elemente haben je nach Hersteller unterschiedliche Bezeichnungen. Anders als im Browser-Umfeld gibt es bei der mobilen Nutzung andere Informationen im Endgerät, die ein Tracking bzw. eine Wiedererkennung des Geräts bzw. der Nutzer:in ermöglichen, so z. B. Advertising- bzw. Werbe-IDs der Store-Anbieter oder Device-Token-IDs für Push-Nachrichten.

THEMEN

→ **Was sagt der Datenschutz**
- Zugriff auf das Endgerät
- Datenverarbeitung
→ Empfehlungen für die Praxis
- Regelmäßiger Check
- Drittanbieter-Cookies
- Einordnung
- Einwilligung
- Datenschutzerklärung

WAS SAGT DER DATENSCHUTZ?

Cookies und vergleichbare Technologien sind auf verschiedenen rechtlichen Ebenen relevant.

ZUGRIFF AUF DAS ENDGERÄT VON NUTZER:INNEN

Insbesondere ist zunächst der Eingriff in das Endgerät der Nutzer:innen zu betrachten, da beim Einsatz von Technologien wie Cookies, Identifiern und Local-Storage-Elementen entsprechende Informationen im Endgerät abgelegt werden bzw. auf gespeicherte Daten und Informationen im Endgerät zugegriffen wird. Der Schutz der Integrität des Endgerätes wird im → **TTDSG** (Telekommunikation-Telemedien-Datenschutz-Gesetz) geregelt. Danach kommt es nicht darauf an, ob die eingesetzten Technologien die Identifizierung der betroffenen Person ermöglichen oder nicht. Es wird auch nicht unterschieden, ob der Eingriff darin besteht, dass Informationen im Endgerät abgelegt werden oder dass auf bereits im Endgerät gespeicherte Informationen zugegriffen wird. Die Regel nach dem TTDSG ist, dass jegliche Eingriffe in das Endgerät der Nutzer:innen einer ausdrücklichen Einwilligung bedürfen. Dies gilt ausnahmsweise nur dann nicht, wenn der Eingriff in das Endgerät **unbedingt erforderlich** ist, damit der Anbieter eines Telemediendienstes einen **vom Nutzer ausdrücklich gewünschten** Telemediendienst zur Verfügung stellen kann. Über die Frage, wann ein Eingriff unbedingt erforderlich ist, wird derzeit auf rechtlicher Ebene diskutiert, weil das TTDSG dazu keine weiteren Anhaltspunkte liefert.

In jedem Fall sind z. B. Cookies, die für den Aufbau einer Website benötigt werden, erforderlich. Auch eine anonymisierte statistische Nutzungsmessung zur Gestaltung eines relevanten öffentlich-rechtlichen Angebotes ist erforderlich (→ **Nutzungsmessung/Tracking**). Entsprechendes gilt für die Speicherung von Einstellungen zur Barrierefreiheit.

Was das Setzen von Cookies für andere, nicht rein funktionale Zwecke, etwa zur Personalisierung, angeht, so ist davon auszugehen, dass eine vorherige Einwilligung der Nutzer:innen einzuholen ist. Die Anforderungen an die Wirksamkeit der Einwilligung richten sich nach den allgemeinen Vorgaben der DSGVO (→ **Datenschutz-‚Basics'**).

DATENVERARBEITUNG

Für die anschließende Verarbeitung von personenbezogenen Daten der Nutzer:innen, die über Cookies und andere Technologien übermittelt wurden, gelten die allgemeinen Regelungen der DSGVO. Dies bedeutet insbesondere auch, dass für die Verarbeitung eine Rechtsgrundlage benötigt wird. So stützt sich beispielsweise die statistische Nutzungsmessung rechtlich auf die Notwendigkeit der staatsvertraglichen Aufgabenerfüllung des öffentlich-rechtlichen Rundfunks.

THEMEN

→ Was sagt der Datenschutz
- Zugriff auf das Endgerät
- Datenverarbeitung
→ **Empfehlungen für die Praxis**
- **Regelmäßiger Check**
- **Drittanbieter-Cookies**
- **Einordnung**
- **Einwilligung**
- **Datenschutzerklärung**

EMPFEHLUNGEN FÜR DIE PRAXIS

REGELMÄSSIGER CHECK

Die Betreiber einer Website sind jeweils für sämtliche über ihre Website gesetzten Cookies verantwortlich, auch wenn diese von Dritten, wie z. B. Auftragsverarbeitern/Drittanbietern stammen. Websites/Apps sollten deshalb regelmäßig auf Cookies/Identifier/Local-Storage-Elemente überprüft werden; hierfür gibt es standardmäßig im Browser integrierte Webmaster-Tools.

DRITTANBIETER-COOKIES KLÄREN

Wenn der Einsatz von Cookies/Identifiern/Local-Storage-Elementen von Auftragsverarbeitern oder Drittanbietern auf der eigenen Website nicht nachvollziehbar ist, muss eine Klärung mit dem Anbieter herbeigeführt werden.

EINORDNEN VON COOKIES/IDENTIFIERN/ LOCAL-STORAGE-ELEMENTEN NACH AKTUELLER RECHTSLAGE

Im Austausch mit den Datenschutzbeauftragten ist zu klären, welche Cookies/Identifier/Local-Storage-Elemente, neben den in diesem Text genannten, nach aktueller Rechtslage als unbedingt erforderlich und damit ggf. als einwilligungsfrei bewertet werden können.

EINWILLIGUNG RICHTIG EINHOLEN

Für alle nicht unbedingt erforderlichen Cookies/Identifier/Local-Storage-Elemente muss die Einwilligung der Nutzer:innen eingeholt werden. Es sind hierzu sichtbare Informationen auf der Startseite, am besten über ein Consent-Management-Tool zu hinterlegen, so dass die Nutzer:innen wissentlich und aktiv (kein vorangekreuztes Kästchen!) über ihre Einwilligungen oder Ablehnungen zu einzelnen oder allen nicht erforderlichen Cookies/Identifiern/Local-Storage-Elementen entscheiden können und zwar vor dem Einsatz auf dem Endgerät. Der Informationstext sollte so konkret wie möglich sagen, um welche Cookies/Identifier/Local-Storage-Elemente es geht, d. h. insbesondere für welche Zwecke diese genutzt werden. Die Einwilligung ist zu protokollieren.

AN DIE DATENSCHUTZERKLÄRUNG DENKEN

In der → **Datenschutzerklärung** oder einer gesonderten Erklärung ist über die eingesetzten Technologien und Möglichkeiten eines jederzeitigen Widerrufs zuvor gegebener Einwilligungen aufzuklären.

NUTZUNGSMESSUNG/ TRACKING

THEMEN

→ **Was sagt der Datenschutz**
- Zugriff auf das Endgerät
- Datenverarbeitung
→ Empfehlungen für die Praxis
- Art und Umfang
- Vertragsverhältnis mit Dienstleister
- Cookie-Blocker
- App-Entwicklung
- Datenschutzerklärung

Unter Nutzungsmessung versteht man die Erhebung von Daten und deren Auswertung zur Analyse des Verhaltens von Nutzer:innen auf Websites oder auch in Apps. Andere Begriffe, die für die Analyse von Nutzerverhalten in der digitalen Welt verwendet werden, sind Web-Analyse, Traffic-Analyse oder Tracking.
Es gibt unterschiedliche Formen der Analyse, die von einer anonymen statistischen Nutzungsmessung bis hin zu komplexen Trackingverfahren reichen, die verschiedene Datenquellen verknüpfen, um Nutzerprofile zu erstellen.
In der Regel wird die Nutzungsmessung von darauf spezialisierten Dienstleistern wie INFOnline, Nielsen, AT Internet etc. über mehrstufige Verfahren durchgeführt. Darüber hinaus gibt es zahlreiche Web-Analyse-Tools wie Google Analytics, Mamoto etc.

WAS SAGT DER DATENSCHUTZ?

ZUGRIFF AUF DAS ENDGERÄT VON NUTZER:INNEN

Um eine Nutzungsanalyse durchführen zu können, werden Technologien eingesetzt, die auf das Endgerät der Nutzer:innen zugreifen, in dem z. B. ein Cookie abgelegt, Local-Storage-Elemente verwendet oder sonstige Geräteinformationen ausgelesen werden. Das heißt, es sind zunächst die Vorgaben des TTDSG zu beachten. (→ **Cookies, Local-Storage-Elemente & Co.**).
Im Falle des Zugriffs auf Endgeräte von Nutzer:innen zur Ermöglichung einer rein statistischen, d. h. anonymisierten Nutzungsmessung ist diese zur Verfügungstellung eines von den jeweiligen Nutzer:innen ausdrücklich gewünschten Dienstes erforderlich und damit der Zugriff auf das Endgerät ohne ausdrückliche Einwilligung des Nutzers/der Nutzerin zulässig. Denn die Analyse der Reichweite und der inhaltlichen Akzeptanz und Präferenz von Angeboten der öffentlich-rechtlichen Rundfunkanstalten ist essenziell, um das Telemedienangebot entsprechend der staatsvertraglichen Vorgaben und in zeitgemäßer Form den Nutzer:innen darzubringen.
Bei erweiterten Formen der Analyse, bei denen neben der rein statistischen Zählung des Zugriffs auf eine Website die Zusammenführung mit anderen Daten der jeweiligen Nutzer:innen,

THEMEN

→ Was sagt der Datenschutz
- Zugriff auf das Endgerät
- **Datenverarbeitung**
→ Empfehlungen für die Praxis
- Art und Umfang
- Vertragsverhältnis mit Dienstleister
- Cookie-Blocker
- App-Entwicklung
- Datenschutzerklärung

also eine Profilbildung erfolgt, ist in der Regel davon auszugehen, dass vor dem dafür erforderlichen Zugriff auf das Endgerät eine ausdrückliche Einwilligung der jeweiligen Nutzer:innen einzuholen ist. Dies gilt insbesondere auch dann, wenn die Nutzungsdaten seitenübergreifend erhoben werden, d. h. nicht nur für das eigene Angebot oder mit den auf den Webseiten Dritter erhobenen Nutzungsdaten zusammengeführt werden sollen. Für die Aspekte der Nutzungsanalyse zum Zwecke der Personalisierung wird auf das Kapitel → **Personalisierung** verwiesen.

DATENVERARBEITUNG

Für die Auswertung der Nutzungsmessung werden personenbezogene Daten, wie etwa die IP-Adresse und in der Regel weitere, zum Teil technische Daten aus dem Browser benötigt, die bei einem Zugriff auf ein Webangebot vom Endgerät an den Server gesendet werden.

Je nach Art der Analyse finden die Verarbeitungsvorgänge bei den beauftragten Dienstleistern statt, die dafür verschiedene Verfahren anwenden. Diese Dienstleister werden in aller Regel als Auftragsverarbeiter für die Rundfunkanstalten tätig, so dass an den Abschluss einer entsprechenden Auftragsverarbeitungsvereinbarung (→ **Auftragsverarbeitung**) zu denken ist.

Bei der anonymisierten statistischen Nutzungsmessung wird die IP-Adresse unmittelbar ‚gehasht' und die weitere Auswertung erfolgt auf Basis von ID-Nummern des Dienstleisters, die von den Rundfunkanstalten keinem/keiner Nutzer:in mehr zugeordnet werden können. Daher wird hier von einer anonymisierten Form der Nutzungsmessung gesprochen. Überdies ist der Eingriff für die Nutzer:innen minimal, da nur sehr wenige personenbezogene Daten (hauptsächlich: IP-Adresse) erhoben und sofort anonymisiert werden. Es ist gut vertretbar, dass diese Form der Nutzungsmessung für die Gestaltung des Angebots, z. B. zur besseren Auffindbarkeit journalistischer Inhalte auf Websites/in Apps, zur Erfüllung des gesetzlichen Auftrags der öffentlich-rechtlichen Rundfunkanstalten gehört. Dies stellt die nach der DSGVO erforderliche Rechtsgrundlage für die Datenverarbeitung dar.

Findet eine darüber hinausgehende Analyse des Nutzungsverhaltens statt und ist, gemessen an der Form und Art des Verfahrens, eine Bezugnahme auf die gesetzliche Aufgabenerfüllung nicht möglich, so können als Rechtsgrundlage für die Datenverarbeitung ein überwiegendes berechtigtes Interesse der Rundfunkanstalt oder die aktive Einwilligung der Nutzer:innen infrage kommen. Da hier allerdings in der Regel bereits der Zugriff auf das Endgerät (s. o.) einer Einwilligung der jeweiligen Nutzer:innen bedarf, ist diese rechtliche Frage hauptsächlich für die weiteren Angaben zu den Nutzerrechten in der → **Datenschutzerklärung** relevant.

THEMEN

→ Was sagt der Datenschutz
- Zugriff auf das Endgerät
- Datenverarbeitung
→ **Empfehlungen für die Praxis**
- **Art und Umfang**
- **Vertragsverhältnis mit Dienstleister**
- Cookie-Blocker
- App-Entwicklung
- Datenschutzerklärung

EMPFEHLUNGEN FÜR DIE PRAXIS

ART UND UMFANG DER NUTZUNGSMESSUNG FESTLEGEN

Die **anonymisierte statistische Nutzungsmessung** ist in der Regel unproblematisch, da nach entsprechender Bewertung keine Einwilligung erforderlich ist (s. o.). Um den Nutzer:innen trotzdem zu ermöglichen, auch diese Form der Nutzungsmessung abzulehnen, kann eine Opt-Out-Möglichkeit vorgesehen werden, über die die Nutzer:innen in einem separaten Fenster oder in der Datenschutzerklärung informiert werden.

Bei **erweiterten Formen der Nutzungsmessung** (z. B. durch Zusammenführung mit weiteren Daten/Prognosen zur Einordnung der Nutzer:innen in Gruppen) ist in der Regel schon für den Zugriff auf das Endgerät des Nutzers/der Nutzerin eine Einwilligung erforderlich, die durch eine entsprechende Information und Abfrage vor dem Zugriff eingeholt werden muss. Zusätzlich bedarf es für die in diesem Zusammenhang vorgenommene Verarbeitung von personenbezogenen Daten einer Rechtsgrundlage. In Betracht kommt ggf. ein berechtigtes Interesse der Rundfunkanstalt (Art. 6 Abs. 1 S. 1 lit. f DSGVO) oder die Einwilligung (→ **Rechtmäßigkeit der Verarbeitung**).

VERTRAGSVERHÄLTNIS MIT DEM DIENSTLEISTER PRÜFEN

In der Regel ist ein Vertrag zur Auftragsverarbeitung mit dem Dienstleister, der die Messung durchführt, abzuschließen (→ **Auftragsverarbeitung**). Der Dienstleister muss auch seine Messmethodik so weit erklären, dass eine datenschutzrechtliche Bewertung des Verfahrens möglich ist. Dies ist z. B. wichtig, um einzuordnen, ob tatsächlich von einer anonymen Messung gesprochen werden kann. Wichtig: Das Vorstehende gilt auch beim Einsatz von Webanalyse-Tools.

THEMEN

→ Was sagt der Datenschutz
- Zugriff auf das Endgerät
- Datenverarbeitung
→ Empfehlungen für die Praxis
- Art und Umfang
- Vertragsverhältnis mit Dienstleister
- **Cookie-Blocker**
- **App-Entwicklung**
- **Datenschutzerklärung**

ACHTUNG COOKIE-BLOCKER

Zu den Messverfahren der Dienstleister gehört auch der Umgang mit Cookie-Blockern, die durch verschiedene Browseranbieter/Anbieter von Betriebssystemen für Smartphones automatisch gesetzt werden und die die Nutzungsmessung, und zwar auch die anonymisierte, erschweren. Die Dienstleister greifen dann in der Regel auf erweiterte Verfahren zurück, etwa indem durch die Verknüpfung mit zusätzlichen, hauptsächlich technischen Daten, die Messgenauigkeit verbessert wird. Finden Änderungen an diesen Verfahren statt, müssen diese mit den Rundfunkanstalten abgestimmt werden. Dabei ist darauf zu achten, dass es bei einer anonymisierten Nutzungsmessung bleibt. In Zweifelsfällen sollte zur Beurteilung der/die Datenschutzbeauftragte hinzugezogen werden.

ACHTUNG APP-ENTWICKLUNG

Bei der Entwicklung von Apps gibt es häufig standardisierte Vorgaben der Dienstleister zum Einbau bestimmter Softwarecodes für die Nutzungsmessung. Hier ist zu prüfen, ob dieser Standard für die Messung der Rundfunkanstalt passt oder ob auf bestimmte Bestandteile, die z. B. für eine Zusammenführung von Nutzerdaten für kommerzielle Zwecke erforderlich wären, zu verzichten ist.

MESSVERFAHREN IN DER DATENSCHUTZERKLÄRUNG/ERKLÄRUNG ZU COOKIES BESCHREIBEN

Die Nutzer:innen sind über die eingesetzten Messverfahren zu informieren, dies gilt insbesondere auch hinsichtlich der Möglichkeiten zum Opt-Out bzw. Widerruf erteilter Einwilligungen.

PERSONALISIERUNG

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Persönliches Nutzerkonto
- Personalisierung über das Endgerät
- Transparenz
- Minderjährigen-Datenschutz

Personalisierung bietet die Möglichkeit, auf Vorlieben und Interessen der Nutzer:innen zugeschnittene Inhalte bereitzustellen. Hierunter fallen z. B. Merklisten, Playlists, Abonnements, Empfehlungen und ‚Weiterschauen'-Funktionen.
Personalisierung kann sehr weit gehen und sich neben den Inhalten auch auf Ansprache, Form, Darstellungsweise und Medium erstrecken. So ist es möglich, die Zeit zum Auffinden von bevorzugten Inhalten zu verkürzen und das Nutzungserlebnis zu verbessern. Davon zu unterscheiden sind Empfehlungen, die ohne Berücksichtigung eines individuellen Nutzungsverhaltens automatisch einem bestimmten Inhalt zugeordnet werden: Beispiel: Im Zusammenhang mit dem Aufruf einer Tatort-Sendung werden in der Mediathek allein durch Verknüpfung der Metadaten der Inhalte stets andere Krimis empfohlen.

WAS SAGT DER DATENSCHUTZ?

Um ein personalisiertes Angebot bereitstellen zu können, werden i. d. R. personenbezogene Daten benötigt. Dies betrifft insbesondere die besonderen Vorlieben und Interessen einer konkreten Person sowie deren Nutzungen. Neben der Möglichkeit, auf explizit angegebene besondere Interessen zurückzugreifen, werden dazu vor allem die Nutzungen bzw. die Nutzungshistorien der Nutzer:innen bzw. die Nutzungen der Endgeräte mithilfe von Algorithmen ausgewertet.

Dazu können personenbezogene Daten aber auch sonstige Daten, die keinen Personenbezug aufweisen, verwendet werden. Werden zur Personalisierung im Endgerät der Nutzer:innen Daten abgelegt oder ausgelesen, was zur ‚Wiedererkennung' stets der Fall sein dürfte, muss neben den Vorschriften zum Datenschutz gemäß DSGVO auch das TTDSG (Telekommunikation-Telemedien-Datenschutz-Gesetz) beachtet werden. (s. unten ‚Empfehlungen für die Praxis' und → **Cookies, Local-Storage-Elemente & Co.**.)

Entscheidend ist, welche Daten in welchem Umfang zu welchem genau definierten Zweck verarbeitet werden, um das mit der Personalisierung verfolgte Ziel zu erreichen. Hier gelten die gleichen Regeln wie bei jeder Datenverarbeitung auch, sodass die in den → **Datenschutz-‚Basics'** dargestellten Grundsätze der Verarbeitung personenbezogener Daten (z. B. Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung) zu beachten sind.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Persönliches Nutzerkonto**
- **Personalisierung über das Endgerät**
- Transparenz
- Minderjährigen-Datenschutz

EMPFEHLUNGEN FÜR DIE PRAXIS

PERSÖNLICHES NUTZERKONTO

Im Rahmen eines Anmeldungsprozesses wird regelmäßig ein Nutzerkonto erstellt. Dazu werden personenbezogene Daten abgefragt und in einer Datenbank hinterlegt. Hier können bereits Vorlieben genannt und eine auf das Angebot bezogene Vorauswahl getroffen werden. Der dafür bereitgestellte Login-Prozess muss datenschutzrechtlichen Anforderungen genügen. Für personalisierte Funktionalitäten sollen nur die Daten der Nutzer:innen erhoben werden, die für die Angebote notwendig, redaktionell intendiert und von den jeweiligen Nutzer:innen gewollt sind. Das Sammeln von Daten auf Vorrat ist unzulässig. Es ist aus Transparenzgründen wichtig, dass das Konto stets von den Nutzenden eingesehen und selbst verwaltet werden kann. Es ist ebenso darüber aufzuklären, dass aus dem Nutzungsverhalten bestimmte Vorlieben herausgelesen werden und eine entsprechende Anpassung des Angebotes daraus folgt. Entscheidend ist auch, dass die so gewonnenen Daten zweckgebunden verarbeitet, sie also nur im Rahmen der vorher erfolgten Aufklärung hinsichtlich des Nutzungszwecks eingesetzt werden. Eine Weitergabe der Daten an Dritte oder andere Stellen – auch innerhalb der Rundfunkanstalten – ist nicht zulässig. Nach Abmeldung des Nutzers/der Nutzerin sind die Daten zu löschen.

PERSONALISIERUNG ÜBER DAS ENDGERÄT

Personalisierung ist auch ohne Einrichtung eines Nutzerkontos möglich. Ein Anmeldeprozess findet in diesem Fall nicht statt. Vielmehr werden durch Zugriff auf Informationen im Endgerät oder durch Speicherung von Informationen im Endgerät der Nutzer:innen deren Nutzungsverhalten ausgelesen und auf dieser Basis ‚dem Endgerät' Empfehlungen gegeben. Dabei werden nicht zwingend personenbezogene Daten erhoben oder das Nutzerverhalten im Backend der Rundfunkanstalt gespeichert.

Eine Einwilligung für diese Art der Personalisierung – oder besser: Individualisierung – muss dessen ungeachtet einholt werden. Das TTDSG erlaubt die Speicherung von Information auf Endgeräten oder auch nur den Zugriff auf dort bereits gespeicherte Informationen auch ohne Personenbezug nur, wenn eine Einwilligung vorliegt, die den Anforderungen der DSGVO genügt (→ **Datenschutz-‚Basics'**). Diese Einwilligung muss vor der Speicherung von Cookies bzw. von Local-Storage-Elementen im Browser und dem Zugriff auf die gespeicherten Informationen vorliegen.

Die Frage, ob im Ausnahmefall auf die Einwilligung verzichtet werden kann, hängt nach den Bestimmungen des TTDSG davon ab, ob die Speicherung von Cookies oder Local-Storage-

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Persönliches Nutzerkonto
- Personalisierung über das Endgerät
- **Transparenz**
- **Minderjährigen-Datenschutz**

Elementen oder der Zugriff auf bereits in dem Gerät gespeicherte Informationen „unbedingt erforderlich“ ist, damit die Rundfunkanstalt einen von den Nutzer:innen ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann. Dies muss in Ansehung des konkreten Vorhabens ggf. mit dem/der Datenschutzbeauftragten der jeweiligen Rundfunkanstalt abgestimmt werden.
Sollten auch bei dieser Art der Personalisierung oder Individualisierung personenbezogene Daten anfallen und ausgewertet werden, bedarf es ebenfalls einer datenschutzkonformen Einwilligung nach DSGVO. Beide Einwilligungserklärungen können zusammen eingeholt werden.

TRANSPARENZ

Bei jeder Art der Personalisierung ist eine umfassende und leicht verständliche Aufklärung über die Datenverarbeitung notwendig. So muss sowohl beim Anmeldeprozess als auch in der Datenschutzerklärung des Angebotes ausführlich über die Möglichkeiten der Personalisierung und die dafür erforderliche Datenverarbeitung informiert werden.

MINDERJÄHRIGEN-DATENSCHUTZ

Werden personalisierte Angebote Minderjährigen direkt gemacht, so ist die Altersgrenze von 16 Jahren zu beachten. Erst ab diesem Alter können Minderjährige selbst einwilligen. Davor kommt es auf die Einsichtsfähigkeit an, sodass eine Einwilligung von 13- bis 16-Jährigen im Regelfall nur mit Zustimmung der Eltern rechtmäßig ist (→ **Minderjährigen-Datenschutz**).

DRITTPLATTFORMEN

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis

Die öffentlich-rechtlichen Rundfunkanstalten verbreiten Programminhalte auch auf Drittplattformen wie Facebook, Instagram, TikTok und YouTube, deren Ausgestaltung sie nicht bestimmen können. Datenschutzrechtlich von Belang sind in erster Linie nicht die dort ausgespielten Inhalte, die unter das → Medienprivileg fallen, sondern die von den Drittplattformen verarbeiteten Nutzerdaten.

WAS SAGT DER DATENSCHUTZ?

Der EuGH hat bereits 2018 in einer Entscheidung zu Facebook festgestellt, dass Fanpage-Betreiber (also diejenigen, die Inhalte über die Plattform verbreiten) für die Datenverarbeitung, die Facebook vornimmt, mitverantwortlich sein können. Die gemeinsame Verantwortung ergibt sich daraus, dass

- es der Drittplattform (hier Facebook) durch die dort platzierten Inhalte ermöglicht wird, Cookies auf den Endgeräten der Nutzer:innen zu platzieren – unabhängig davon, ob die Personen über ein Konto bei dieser Plattform verfügen,
- der Betreiber einer Präsenz auf der Plattform (die Rundfunkanstalt) die Kriterien von Auswertungsstatistiken seiner Seiten für die Drittplattform bestimmen kann und damit unmittelbar auf die Datenauswertung der Plattform einwirken kann,
- die Rundfunkanstalt verlangen kann, dass ihr demografische Daten ihrer Zielgruppen mitgeteilt werden; dies gilt auch, wenn diese Mitteilung anonymisiert erfolgt, ihr aber eine personenbezogene Datenerhebung durch die Plattform vorgeschaltet ist.

Die im EuGH-Urteil getroffenen Feststellungen sind auch auf andere Drittplattformen übertragbar. Wenn diese drei Voraussetzungen vorliegen, muss von einer gemeinsamen datenschutzrechtlichen Verantwortung der Rundfunkanstalten mit den Drittplattformbetreibern ausgegangen werden.
Daraus ergibt sich die Pflicht zum Abschluss eines sogenannten → **Joint-Controller-Vertrages** (Art. 26 DSGVO), der Art und Umfang der Verantwortung für die einzelnen personenbezogenen Datenverarbeitungen abgrenzt und Absprachen darüber trifft, welcher Vertragspartner die Erfüllung welcher Pflichten nach der DSGVO zu übernehmen hat.

Problematisch ist bei dieser Fallkonstellation, dass die Rechtmäßigkeit der Datenverarbeitung von vielen großen Plattformen (z. B. Facebook im Hinblick auf mangelnde Transparenz und Datenübermittlungen in die USA, oder TikTok hinsichtlich der unklaren Sachlage bzgl. einer Datenübermittlung nach Chi-

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis

na) zweifelhaft ist, und die Plattformen auch von Nutzer:innen besucht werden, die nicht dort angemeldet sind und ggf. nicht in die Datenverarbeitung eingewilligt haben. Im Ergebnis muss vor der Entscheidung für eine Präsenz der Rundfunkanstalt auf Drittplattformen wie Facebook & Co. immer eine Abwägung des staatsvertraglichen Programmauftrags, zeitgemäße Telemedien anzubieten, mit den betroffenen Nutzerrechten erfolgen. Im Hinblick darauf, dass der öffentlich-rechtliche Rundfunk keine wirtschaftlichen Interessen verfolgt und mit der Einrichtung von solchen Web-Präsenzen insbesondere für Nachrichtensendungen seinen Programmauftrag im Internet wahrnimmt, muss im Einzelfall eine Entscheidung getroffen werden, die allen Belangen Rechnung trägt.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**

EMPFEHLUNGEN FÜR DIE PRAXIS

› Zunächst sollte dokumentiert werden, aus welchen Gründen eine Präsenz auf der jeweiligen Plattform angestrebt wird. Ist die Datenverarbeitung der Drittplattform nach europäischen Maßstäben nicht sicher rechtskonform und ist von einer gemeinsamen Verantwortung auszugehen, so droht das Risiko, dass sich die jeweils zuständige Aufsichtsbehörde (Rundfunkdatenschutzbeauftragte:r) an die Rundfunkanstalt wendet und die Rechtsmäßigkeit der Präsenz auf einer Drittplattform aus datenschutzrechtlichen Gründen anzweifelt. Hierbei sind die publizistischen Argumente mit dem auf der Plattform vorzufindenden Datenschutzniveau abzuwägen. Es ist darauf zu achten, dass Inhalte nicht ausschließlich auf Drittplattformen verbreitet werden, damit Nutzer:innen nicht gezwungen sind, die Inhalte dort abzurufen.

› Es muss anhand oben genannter Kriterien geprüft werden, ob eine gemeinsame Verantwortung für die Verarbeitung der Nutzerdaten besteht; in diesem Fall hat die Rundfunkanstalt mit dem Betreiber der Drittplattform eine sogenannte → **Joint-Controller-Vereinbarung** nach Artikel 26 DSGVO abzuschließen, aus der u. a. der Grad der jeweiligen Verantwortlichkeit hervorgehen muss. Unter Umständen stellen die Plattformen solche Verträge in Form von AGB zur Verfügung (z. B. das Facebook-Addendum), deren Vollständigkeit und Rechtmäßigkeit mit den betrieblichen Datenschutzbeauftragten geprüft und besprochen werden sollte.

› Überdies müssen die Rundfunkanstalten festhalten, auf welcher Rechtsgrundlage die von ihnen verantwortete Verarbeitung der Nutzerdaten (z. B. zum Zweck der Nutzungsmessung) fußt. In Betracht kommt hier vor allem Artikel 6 Abs. 1 S. 1 lit. e DSGVO, da die Datenverarbeitung im Rahmen der Aufgabenerfüllung erfolgt (→ **Nutzungsmessung/Tracking**).

› In einer Datenschutzerklärung hat die verantwortliche Rundfunkanstalt ihren Informationspflichten nach den Artikeln 13, 14 DSGVO nachzukommen. Im Fall der gemeinsamen Verantwortlichkeit ist darzulegen, welche Daten zu welchem Zweck von welchen Verantwortlichen verarbeitet werden. Hier muss ebenso auf die Datenschutzerklärung der Plattform verwiesen werden und möglichst detailliert erläutert werden, welche Datenkategorien im Interesse der Anstalt verarbeitet werden. Dies ist auch dann der Fall, wenn den Anstalten von den Plattformen lediglich anonymisierte Daten und Statistiken zur Verfügung gestellt werden.

EMBEDDING VON FREMDINHALTEN

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Einbettung erforderlich?
- Einbettung mit Auftragsverarbeitung?
- Zwei-Click-Lösung
- Social Plugins
- Datenschutzerklärung
- Blog-/Kuratiertools

Embedding bedeutet das Einbetten fremder Inhalte in eigene Websites oder Apps. Eingebettet werden z. B. Fotos, Grafiken, Audio- und Videofiles, Textnachrichten sowie Social Plugins zum Teilen und Liken von Inhalten. Während die Rundfunkanstalten z. B. Tools von Kartenanbietern zur Ergänzung ihres Angebotes nutzen oder sich im Rahmen ihres Funktionsauftrags mit Originalquellen von anderen Anbietern publizistisch auseinandersetzen, dienen die Social Plugins dazu, den Angeboten der Rundfunkanstalten eine höhere Reichweite zu verschaffen. Das Einbinden fremder Inhalte wird dabei häufig über sog. iFrames (Inlineframes) realisiert. Einfach gesprochen ist der iFrame ein ‚kleines Fenster', in dem eine externe Website, die auf einem anderen Server liegt, angezeigt wird.

Bereits beim Aufrufen einer Website oder App der Rundfunkanstalt, auf der Inhalte Dritter eingebettet sind, werden regelmäßig die IP-Adresse sowie weitere gerätebezogene Informationen der Nutzer:innen an die Drittanbieter übertragen. Außerdem eröffnet das Aufrufen einer Website mit eingebetteten Inhalten den Drittanbietern die Möglichkeit, Cookies auf den Geräten der Nutzer:innen zu platzieren.

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Einbettung erforderlich?
- Einbettung mit Auftragsverarbeitung?
- Zwei-Click-Lösung
- Social Plugins
- Datenschutzerklärung
- Blog-/Kuratiertools

WAS SAGT DER DATENSCHUTZ?

Erfolgt die durch das Embedding ausgelöste Datenverarbeitung beim Drittanbieter ausschließlich zur Bereitstellung der Inhalte im Auftrag und nach Weisung der Rundfunkanstalt, so ergeben sich keine Besonderheiten. Die Rundfunkanstalt ist für die Datenverarbeitung nach außen allein verantwortlich. In einer Vereinbarung zur Auftragsverarbeitung muss die Rundfunkanstalt die Art und Weise der Datenverarbeitung mit dem Drittanbieter konkret festlegen und die Verwendung der Daten für eigene Zwecke des Drittanbieters ausschließen. Es gelten die Hinweise zur → **Auftragsverarbeitung**. Für die Einbindung von Inhalten durch Auftragsverarbeiter und die damit verbundene Verarbeitung von Nutzerdaten beim Auftragnehmer ist keine Einwilligung der Nutzer:innen erforderlich. Im Rahmen eines Auftragsverarbeitungsverhältnisses werden aktuell z. B. Tools von Kartenanbietern (z. B. Bing-Maps) in die Angebote der Rundfunkanstalten eingebunden. Rechtlich problematisch kann hingegen das Einbetten fremder Inhalte außerhalb eines Auftragsverarbeitungsverhältnisses sein. Denn ohne besondere Vorkehrungen veranlasst die Rundfunkanstalt auch in diesem Fall durch das bloße Einbetten der Inhalte, dass bereits beim Aufrufen ihrer Website oder App mit eingebetteten Inhalten automatisch die IP-Adresse sowie weitere gerätebezogene Informationen der Nutzer:innen an die Drittanbieter übertragen werden. Im Unterschied zur Datenverarbeitung im Rahmen eines Auftragsverarbeitungsverhältnisses kann die Rundfunkanstalt nicht verhindern, dass die Drittanbieter diese Daten auch zu eigenen (wirtschaftlichen) Zwecken nutzen und durch die Platzierung von Cookies auf den Geräten der Nutzer:innen zusätzlich deren individuelles Surfverhalten erfassen. Soweit keine zusätzlichen Schutzvorkehrungen getroffen werden, geschieht dies, ohne dass die Nutzer:innen das eingebettete Angebot überhaupt angeklickt haben und ohne beim jeweiligen Anbieter(z. B. Twitter) eingeloggt zu sein.

Nach der Rechtsprechung des EuGH (‚Fashion ID'-Urteil) können die Rundfunkanstalten – wenn sie keine Vorkehrungen treffen – für die durch das Embedding veranlasste Verarbeiten personenbezogener Daten und das Setzen von Cookies durch Drittanbieter rechtlich mitverantwortlich sein. Dies hätte zur Folge, dass sie einen sog. → **Joint-Controller-Vertrag** mit dem jeweiligen Drittanbieter schließen müssten, in welchem die Verantwortlichkeiten für die einzelnen Verarbeitungsstufen klar voneinander abgegrenzt werden (→ **Datenschutz-‚Basics'**).

Um eine Mitverantwortung zu vermeiden, müssen die Rundfunkanstalten technisch dafür sorgen, dass bei Aufruf der Website die fremden Inhalte zunächst inaktiv sind. Die Datenübertragung an die Drittanbieter darf erst erfolgen, wenn sich die Nutzer:innen aktiv dafür entscheiden und die Datenübertragung eigenverantwortlich auslösen. Über diesen Umstand müssen die Nutzer:innen zuvor explizit aufgeklärt werden.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Einbettung erforderlich?**
- **Einbettung mit Auftragsverarbeitung?**
- Zwei-Click-Lösung
- Social Plugins
- Datenschutzerklärung
- Blog-/Kuratiertools

EMPFEHLUNGEN FÜR DIE PRAXIS

EINBETTUNG AUS REDAKTIONELLEN GRÜNDEN ERFORDERLICH?

Beim Einbetten von externen Inhalten sollte zunächst der redaktionelle Mehrwert der Verwendung der Inhalte gegen die datenschutzrechtlichen Risiken im Einzelfall abgewogen werden. Entscheidend ist der durch die Einbettung ausgelöste Umfang der Datenverarbeitung durch den Drittanbieter. Zu prüfen ist auch, ob beim Drittanbieter die Möglichkeit datenschutzfreundlicher Voreinstellungen gegeben ist. Beispielsweise bieten einzelne Drittanbieter durch den erweiterten Datenschutzmodus die Möglichkeit an, Cookies von Beginn an auszuschalten. Hinweise dazu geben die jeweiligen Datenschutzrichtlinien bzw. Nutzungsbedingungen der Drittanbieter. Zu berücksichtigen ist, dass viele Drittanbieter nicht transparent und vollständig über die Datenverarbeitung aufklären.

ERFOLGT DIE EINBETTUNG IM RAHMEN EINER DATENSCHUTZRECHTLICHEN AUFTRAGSVERARBEITUNG?

Überwiegt der redaktionelle Mehrwert, sollte als nächstes geprüft werden, ob die Einbettung der Inhalte im Wege einer datenschutzrechtlichen Auftragsverarbeitung erfolgt. In diesem Fall muss mit dem Drittanbieter eine Vereinbarung zur Auftragsverarbeitung geschlossen werden, in der die Verarbeitung der Nutzerdaten konkret festgelegt und die Verwendung der Daten zu eigenen Zwecken durch den Drittanbieter ausgeschlossen wird (→ **Auftragsverarbeitung**).

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Einbettung erforderlich?
- Einbettung mit Auftragsverarbeitung?
- **Zwei-Click-Lösung**
- **Social Plugins**
- Datenschutzerklärung
- Blog-/Kuratiertools

EINSATZ DER (MODIFIZIERTEN) ZWEI-KLICK-LÖSUNG

Falls die Einbettung nicht im Rahmen einer Auftragsverarbeitung erfolgt, muss sichergestellt werden, dass personenbezogene Daten erst dann an den Drittanbieter übermittelt werden, wenn sich die Nutzer:innen aktiv dafür entschieden haben. Bei der Zwei-Klick-Lösung sind die fremden Inhalte bei Aufruf der Onlineseite der Rundfunkanstalt zunächst inaktiv. Erst nach der Aktivierung einer Zwischenschaltfläche durch die Nutzer:innen beginnt die Datenübertragung.

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

Für Tweets, Bilder oder Videos kann auch die Open-Source-Technik embetty verwendet werden. Auch dabei werden zunächst keine Daten übertragen. Die Nutzer:innen können die jeweilige Website besuchen, ohne dass gleichzeitig ihr Surfverhalten für die sozialen Netzwerke sichtbar wird. Die Daten der Nutzer:innen werden zunächst auf einem Zwischenserver gespeichert. Die Verbindung zum sozialen Netzwerk wird erst dann hergestellt, wenn die Nutzer:innen aktiv werden und auf einen entsprechenden Button klicken. Der Vorteil dieser Lösung ist, dass es nur einen Button gibt.

SOCIAL PLUGINS

Auf Social Plugins, wie z. B. für das Teilen oder Liken auf Facebook, Twitter und Instagram, sollte verzichtet werden. Stattdessen sollte auf die entsprechenden Funktionen beim Anbieter verlinkt werden. Mit der Aktivierung des Links verlassen die Nutzer:innen die Sphäre der Rundfunkanstalt und begeben sich in den Verantwortungsbereich des Drittanbieters. Eine andere Möglichkeit ist die Nutzung des sog. Shariff-Buttons, der ähnlich wie embetty funktioniert.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Einbettung erforderlich?
- Einbettung mit Auftragsverarbeitung?
- Zwei-Click-Lösung
- Social Plugins
- **Datenschutzerklärung**
- **Blog-/Kuratiertools**

INFORMATION ÜBER DAS EMBEDDING VON INHALTEN UND TOOLS VON DRITTANBIETERN IN DER DATENSCHUTZERKLÄRUNG

Die Rundfunkanstalten müssen in ihren Datenschutzerklärungen umfassend über das Einbinden von externen Inhalten und Social Plugins auf ihren Websites informieren. Die Hinweise sollten nach Drittanbietern differenziert werden. Dabei sollte auch auf die Zwei-Klick- und andere Lösungen Bezug genommen und die Funktionsweise erläutert werden.

EXKURS: BLOG-/KURATIERTOOLS

Blog-/Kuratiertools sind Werkzeuge, die die Rundfunkanstalten zur Erzeugung ihrer eigenen Inhalte und Integration von Social-Media-Kanälen verwenden. In der Regel fließen hier Daten zum Dienstleister. 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 der Nutzer:innen gesetzt.

Die Verarbeitung der Nutzerdaten beim Dienstleister des Tools geschieht im Wege der Auftragsverarbeitung. Die Datenverarbeitung wird der Rundfunkanstalt zugerechnet. Es gelten hier die Hinweise zur → **Auftragsverarbeitung**. Mit der Vereinbarung zur Auftragsverarbeitung muss insbesondere sichergestellt werden, dass der Drittanbieter die Nutzerdaten nicht für eigene Zwecke verwendet. 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.

SOCIAL LOGIN

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Integration erforderlich?
- Information und Einwilligung
- Aufklärung
- Alternativen

Bestimmte Funktionen im Zusammenhang mit der Nutzung von Telemedienangeboten der Rundfunkanstalten, z. B. die Personalisierung oder die Teilnahme an einem Gewinnspiel, setzen eine Registrierung voraus. Um den Registrierungsprozess zu erleichtern, bieten die Rundfunkanstalten den Nutzer:innen mitunter an, sich mit ihren Accounts aus sozialen Netzwerken wie Facebook und Twitter anzumelden. Dies wird als Social Login bzw. Social Sign-In bezeichnet. Den Nutzer:innen erspart dies, sich zusätzliche Passwörter merken zu müssen. Außerdem ist dadurch ein nahtloser Übergang zwischen den Angeboten der Rundfunkanstalten und den Social Media möglich.

WAS SAGT DER DATENSCHUTZ?

Durch die Registrierung mit einem Social Login erhält die Rundfunkanstalt personenbezogene Daten der Nutzer:innen von den sozialen Netzwerken. Die sozialen Netzwerke erhalten ihrerseits personenbezogene Daten der Nutzer:innen.
Sie erhalten die Möglichkeit, Cookies und andere Identifier auf den Geräten der Nutzer:innen abzulegen, um weitere Informationen über das Nutzungsverhalten zu erlangen. Die Nutzungsdaten können dem Benutzerprofil der sozialen Netzwerke beigefügt und von diesen weiterverarbeitet werden (z. B. Auswertung der Daten zu Werbezwecken). Dafür ist die Einwilligung der Nutzer:innen erforderlich.

Zu beachten ist, dass für das Social Login dieselbe Technik wie beim → **Embedding** zum Einsatz kommt. In der Konsequenz erhalten die sozialen Netzwerke bereits beim bloßen Aufrufen einer Website, auf der die Möglichkeit eines Social Login implementiert ist, Informationen zum Surfverhalten der Nutzer:innen. Betroffen sind alle Nutzer:innen, also auch diejenigen, die gar nicht bei den sozialen Netzwerken registriert sind.

Um dies zu vermeiden, muss die Rundfunkanstalt vor das Social Login einen Vorschaltbutton setzen. Bevor dieser von den Nutzer:innen angeklickt werden kann, muss die Rundfunkanstalt konkret über die durch das Social Login ausgelöste Datenverarbeitung aufklären und dafür eine explizite Einwilligung einholen. Möglich ist eine Verlinkung auf die Datenschutzerklärung der sozialen Netzwerke.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlung für die Praxis**
- **Integration erforderlich?**
- **Information und Einwilligung**
- Aufklärung
- Alternativen

EMPFEHLUNGEN FÜR DIE PRAXIS

INTEGRATION VON SOCIAL LOGIN ERFORDERLICH?

Zunächst sollte sorgfältig geprüft werden, ob ein Social Login überhaupt sinnvoll und notwendig ist. Die Integration von Log-in-Funktionen von sozialen Netzwerken ist – wie dargestellt – problematisch, weil sie mit den einzuhaltenden Grundsätzen der Datensparsamkeit und Transparenz kollidiert.

Als sog. ID-Provider für das Login treten auch Firmen auf, die keine sozialen Netzwerke betreiben, z. B. Apple, Microsoft und Google. Allerdings sammeln auch diese ID-Provider Nutzerdaten und sollten daher nach Möglichkeit nicht angeboten werden.

Seit 2020 können ARD- und ZDF-Logins wechselseitig verwendet werden. Bei der ARD registrierte Nutzer:innen können also mit ihrem Login auch die personalisierten Funktionen des ZDF nutzen und umgekehrt. Aus Datenschutzsicht ist eine gemeinsame Login-Sphäre mit anderen öffentlich-rechtlichen Anbietern dem Social Login vorzuziehen.

INFORMATION UND EINWILLIGUNG UNMITTELBAR BEIM SOCIAL LOGIN

Soll der Social Login dennoch angeboten werden, so ist ein Vorschaltbutton zu verwenden. Vor Betätigung des Vorschaltbuttons müssen die Nutzer:innen darüber informiert werden, welche Daten die Rundfunkanstalt von dem sozialen Netzwerk für welchen Zweck erhält und welche Daten zu welchem Zweck an das soziale Netzwerk übermittelt werden, und dem aktiv zustimmen. Für die Einholung der Einwilligung sollte auf die Datenschutzerklärung der sozialen Netzwerke verlinkt werden. Den Nutzer:innen sollte auch erklärt werden, wie die Verknüpfung zwischen der Website der Rundfunkanstalt und den sozialen Netzwerken wieder gelöst werden kann.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Integration erforderlich?
- Information und Einwilligung
- Aufklärung
- Alternativen

AUFKLÄRUNG ZUM SOCIAL LOGIN IN EIGENER DATENSCHUTZERKLÄRUNG

Über das Social-Login-Verfahren und die dabei ablaufenden Datenverarbeitungsprozesse sollte auch in der allgemeinen Datenschutzerklärung der Rundfunkanstalt aufgeklärt werden.

ALTERNATIVE REGISTRIERUNGS-MÖGLICHKEIT

In jedem Fall muss den Nutzer:innen immer freigestellt werden, zwischen dem Social Login und einer separaten Registrierungsmöglichkeit frei zu wählen. Aus Wettbewerbsgründen müssen immer mindestens zwei verschiedene Social-Login-Möglichkeiten zur Verfügung gestellt werden.

INSTANT MESSAGING

THEMEN

→ **Was sagt der Datenschutz**
→ Empfehlungen für die Praxis
- Nutzung erforderlich?
- Datenschutzrelevante Aspekte prüfen
- Datenschutzerklärung
- Löschung
- Alternative Kommunikationswege
- Minderjährigen-Datenschutz

Neben den klassischen Sozialen Netzwerken spielt das sog. Instant Messaging als Rückkanal für die Zuschauer:innen und -hörer:innen z. B. bei der Durchführung von Gewinnspielen eine große Rolle. Die Rundfunkanstalten nutzen das Instant Messaging auch als Plattform, über die redaktionelle Inhalte verbreitet werden. Populäre Instant-Messaging-Dienste sind aktuell z. B. WhatsApp, Telegram, Signal und Threema.
Beim Instant Messaging löst der/die Absender:in die Datenübermittlung aus (sog. ‚Push-Verfahren'), so dass die Nachrichten (fast) unmittelbar (englisch ‚instant') bei den Empfänger:innen ankommen. Viele Instant-Messenger unterstützen zusätzlich die Übertragung von Dateien sowie Audio- und Video-Streams. Nutzer:innen können sich gegenseitig in ihrer Kontaktliste führen und sehen dann an der Präsenzinformation, ob andere zu einem Gespräch bereit sind.

WAS SAGT DER DATENSCHUTZ?

In datenschutzrechtlicher Hinsicht ist zunächst problematisch, dass ein Teil der Messenger-Dienste (z. Zt. z. B. WhatsApp und Signal) automatisch regelmäßig auf sämtliche Kontakte in den Adressbüchern des jeweiligen Endgeräts zugreift und diese mit eigenen Nutzerdaten abgleicht, um ermitteln zu können, mit welchem Kontakt eine Kommunikation möglich ist. Viele Messenger-Anbieter informieren die Nutzer:innen nicht oder unzureichend über ihre Datenschutzbestimmungen. Ein Teil der Messenger-Dienste verzichtet auf eine Ende-zu-Ende-Verschlüsselung. So können Inhalte, Kontakte und andere vertrauliche Daten von Unbefugten ausgelesen werden. Beim zu Meta (ehemals Facebook) gehörenden Messenger-Dienst WhatsApp muss damit gerechnet werden, dass Daten innerhalb des Meta-Konzerns auch mit anderen, zum Konzern gehörenden Diensten wie dem sozialen Netzwerk Facebook und der Video- und Foto-Sharing-App Instagram zu Werbezwecken ausgetauscht werden. Schließlich ist zu beachten, dass ein Teil der Messenger-Dienste (z. B. WhatsApp) seine Server in den USA betreibt, was derzeit problematisch ist (→ **Datenschutz-‚Basics'**). Auch wenn dortige Sicherheitsbehörden wegen der Ende-zu-Ende -Verschlüsselung nicht auf die Inhalte der Kommunikation selbst zugreifen können, sind z. B. die Rufnummern und Daten aus Adressbüchern nur unzureichend vor einem Zugriff der staatlichen Stellen geschützt.

THEMEN

→ Was sagt der Datenschutz
→ **Empfehlungen für die Praxis**
- **Nutzung erforderlich?**
- **Datenschutzrelevante Aspekte prüfen**
- **Datenschutzerklärung**
- **Löschung**
- Alternative Kommunikationswege
- Minderjährigen-Datenschutz

EMPFEHLUNGEN FÜR DIE PRAXIS

NUTZUNG VON MESSENGER-DIENSTEN ERFORDERLICH?

Mit Blick auf die vorgenannten Datenschutzprobleme sollte der Einsatz redaktionell gut begründet und dokumentiert sein. Die Nutzung eigener Plattformen (z. B. der Radio-Apps) als Rückkanal und zum Verbreiten von Informationen sollte möglichst vorgezogen werden.

DATENSCHUTZRELEVANTE ASPEKTE PRÜFEN

Bei der Auswahl von Messenger-Diensten ist darauf zu achten, dass ein automatisches Auslesen von Adressdaten ausgeschlossen und die Kommunikation Ende-zu-Ende-verschlüsselt ist. Anbieter mit Serverstandorten innerhalb der EU sind nach Möglichkeit zu bevorzugen. Außerdem sollte darauf geachtet werden, dass nur eine lokale Speicherung der Daten auf dem Gerät vorgenommen wird und keine automatische Synchronisation mit Drittanbietern erfolgt.

INFORMATION IN DATENSCHUTZERKLÄRUNG

In der allgemeinen Datenschutzerklärung müssen die Nutzer:innen über den Einsatz von Instant Messengers durch die Rundfunkanstalt informiert werden.

AN DIE LÖSCHUNG DENKEN

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Personenbezogene Nutzerdaten (z. B. Einsendungen im Rahmen eines Gewinnspiels) müssen grundsätzlich nach Zweckerfüllung gelöscht werden. Eine Löschung ist nicht erforderlich, wenn die Daten anonymisiert werden. Werden Einsendungen für programmliche Zwecke genutzt (z. B. Fotos oder Geschichten), gilt insoweit das → **Medienprivileg** mit der Folge, dass die Einsendungen auch länger archiviert werden können. Zu beachten ist die gesetzliche Aufzeichnungspflicht für Rundfunksendungen.

THEMEN

→ Was sagt der Datenschutz
→ Empfehlungen für die Praxis
- Nutzung erforderlich?
- Datenschutzrelevante Aspekte prüfen
- Datenschutzerklärung
- Löschung
- **Alternative Kommunikationswege**
- **Minderjährigen-Datenschutz**

ALTERNATIVE DATENSCHUTZKONFORME KOMMUNIKATIONSWEGE

Für die Nutzer:innen sollten auch immer alternative datenschutzfreundliche Kommunikationswege angeboten werden.

MINDERJÄHRIGEN-DATENSCHUTZ

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

Leitlinien zum Datenschutz in den Telemedien-Angeboten von ARD, ZDF und Deutschlandradio

2., vollständig überarbeitete Auflage (Dezember 2021)

Herausgeber: Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio

Koordination der Redaktion: Anke Naujock-Simon, Datenschutzbeauftragte des Rundfunk Berlin-Brandenburg

Design: dot_agentur, Matthias Schröppel