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

Herausgeber: Arbeitskreis der Datenschutzbeauftragten
von ARD, ZDF und Deutschlandradio

Inhalt

VORBEMERKUNG

Was will Datenschutz?

Datenschutz ist ein Grundrecht, das die Privatsphäre schützt.

Freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen unbegrenzte Erhebung, Verarbeitung und Weitergabe seiner personenbezogenen Daten voraus. Datenschutz ist das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (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 stellen den Datenschutz dabei vor neue Herausforderungen. Das Wachstum des Internets geht mit einem stetigen Anstieg der gesammelten personenbezogenen Daten einher.

Was will der Leitfaden?

Dieser Leitfaden ist ein Ratgeber und richtet sich an die Mitarbeiter[1], die Telemedien- und Social-Media-Angebote redaktionell einsetzen und technisch realisieren. Er konkretisiert die verbindlichen Vorgaben der Datenschutzgesetze und der einschlägigen Rechtsprechung für öffentlich-rechtliche Telemedien- und Social-Media-Angebote.

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

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

1 Zur besseren Lesbarkeit wird im Folgenden ausschließlich eine Bezeichnungsform verwendet. Selbst-verständlich sind alle Formulierungen für alle Geschlechter gleichermaßen zutreffend.

DATENSCHUTZ „BASICS“

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

Sind die Daten personenbezogen?

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

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Darunter versteht man alle Daten, die dazu genutzt werden können, die Identität des Users offen zu legen. Dazu gehören nicht nur der richtige Name, Anschrift, Telefonnummer oder eine E-Mail-Adresse. Auch andere Informationen wie z.B. die IP-Adresse, Standortdaten, Gerätekennungsnummern sowie sonstige Informationen (z.B. über das Nutzungsverhalten) sind ebenfalls relevant, weil sie zumindest personenbeziehbar sind.[2]

Wer ist die für die Datenverarbeitung „verantwortliche Stelle“?

Wenn die Rundfunkanstalt in ihren Telemedienangeboten personenbezogene Daten von Nutzern verarbeitet, ist sie gemäß den Datenschutzgesetzen die „verantwortliche Stelle“ und damit verantwortlich für die datenschutzkonforme Gestaltung ihrer Angebote.

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

2 Aufgrund der aktuellen Rechtsprechung und im Einklang mit der Auffassung der deutschen Aufsichtsbehörden im Datenschutz sind statische und dynamische IP-Adressen als personen-bezogene Daten zu werten.

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

Ist die Rundfunkanstalt auf einer Drittplattform präsent, ist grundsätzlich der jeweilige Plattformanbieter für die Datenverarbeitung datenschutzrechtlich verantwortlich (siehe hierzu die Hinweise zu ***Drittplattformen***).[3]

Rechtmäßigkeit der Datenerhebung und -nutzung

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

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

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

Einwilligung des Nutzers

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

» Der Nutzer ist vor Beginn der Datenverarbeitung umfassend zu informieren.

» Der Text der Einwilligungserklärung muss dem Nutzer klar und allgemein verständlich über die zu

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

verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die Rundfunkanstalt informieren.

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

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

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

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

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

» Die Einwilligung muss jederzeit in einfacher Weise vom Nutzer widerrufbar sein. Der Nutzer ist über sein Widerrufsrecht zu informieren. Die Unterrichtung kann z.B. in der allgemeinen ***Datenschutzerklärung*** erfolgen.

» Die datenschutzrechtliche Einwilligung zu einer konkreten Datenverarbeitung ist deutlich zu trennen von den generellen Datenschutzhinweisen in einem Telemedienangebot mit reinen Informationen über Datenverarbeitung auf gesetzlicher Grundlage (siehe hierzu die Hinweise zur ***Datenschutzerklärung***).

» Besonderheiten gelten bei der Datenverarbeitung von Minderjährigen (Hinweise zum ***Minderjährigen-Datenschutz***).

Grundsatz der Zweckbindung und Erforderlichkeit

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

Sobald die personenbezogenen Daten nicht mehr zu dem ursprünglich angegebenen Zweck

benötigt werden, müssen sie grundsätzlich gelöscht werden. Das gleiche gilt im Falle des Widerrufs einer Einwilligungserklärung in die Datenverarbeitung durch den Nutzer.

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

Grundsatz der Datenvermeidung und Datensparsamkeit

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

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

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

„Privacy by Design“ und „Privacy by Default“

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

Transparenz

Das Grundrecht auf informationelle Selbstbestimmung verlangt: Der Einzelne soll wissen, wer

was wann und bei welcher Gelegenheit über ihn weiß. Das Transparenzprinzip wirkt sich an vielen Stellen im Datenschutzrecht aus:

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

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

Datensicherheit

IT-Systeme sind aufgrund ihrer Komplexität anfällig für Fehler, über die z.B. Unbefugte an Daten gelangen können. Gleichzeitig werden auch die Angriffe auf technische Systeme immer häufiger und ausgefeilter. Die Rundfunkanstalt hat daher gemeinsam mit dem IT-Sicherheitsbeauftragten und/oder der zuständigen Fachabteilung für ihre Webseiten und Apps geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Daten ihrer Nutzer gegen Verfälschung, Verlust und Missbrauch zu schützen.

APPS

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

Was sagt der Datenschutz?

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

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

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

Checkliste

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

× Welche personenbezogenen Daten werden genutzt?

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

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

× „Privacy by Design“ und „Privacy by Default“

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

× Möglichkeit der anonymen und pseudonymen Nutzung

Soweit es möglich ist, sollte die Rundfunkanstalt die Nutzung ihrer App anonym oder unter

Pseudonym ermöglichen. Über diese Möglichkeit ist der Nutzer zu informieren. Achtung: Eindeutige Geräte- und Kartenkennungen oder die IP-Adresse stellen kein Pseudonym dar!

× Berechtigungen nur nach dem Grundsatz der Zweckbindung

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

Hier gilt: Es dürfen nur die für die App tatsächlich erforderlichen Berechtigungen vom Nutzer angefordert werden. Einige Betriebssysteme bieten Berechtigungen nur in festen Kombinationen an, welche neben der erforderlichen Berechtigung auch nicht benötigte Berechtigungen enthalten. Die Rundfunkanstalt muss in der Datenschutzerklärung über diesen Umstand aufklären und sich gegenüber dem Nutzer dazu verpflichten, von der nicht erforderlichen Berechtigung keinen Gebrauch zu machen.

× Es gilt: Grundsatz der Einwilligung

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

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

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

× Erlaubt: Pseudonyme Nutzungsprofile unter bestimmten Voraussetzungen

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

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

× Push-Funktionen mit Zustimmung des Nutzers zulässig

Mit der Push-Funktion können verschiedene Inhalte - z.B. Kurznachrichten, Live-Ticker usw.

- von einem Server zu einem speziellen Mobilgerät versandt werden. Hat der Nutzer einmal den Dienst abonniert, übernimmt der Server eigeninitiativ das „Pushen“ des Inhalts zum Nutzer-Device.

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

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

× Achtung bei Standortdaten

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

× Achtung beim Einbinden von Inhalten von Drittanbietern

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

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

× Umfassende spezifische Datenschutzerklärung vor Installation der App

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

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

Eine einfache Verknüpfung mit der Datenschutzerklärung eines ähnlichen oder alternativen Webangebotes der Rundfunkanstalt genügt dann nicht, wenn es hinsichtlich der

Datenverarbeitung relevante Unterschiede bei der Datenverarbeitung einer Webseite und einer App gibt.

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

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

× Auf Datensicherheit achten

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

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

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

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

× Achtung bei Beauftragung von Dritten

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

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

Im Übrigen gelten die Hinweise zur ***Auftragsvergabe an Dritte***.

× Minderjährigen-Datenschutz

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

AUFTRAGSVERGABE AN DRITTE

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

Was sagt der Datenschutz?

Vorab ist gemeinsam mit dem Datenschutzbeauftragten zu klären, ob es sich um eine sog. Auftragsdatenverarbeitung i.S. des Datenschutzrechts handelt.

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

Checkliste

× Grundsätzlich: Bevorzugung einer „Inhouse"-Lösung

Eine Vergabe von Aufträgen an Externe ist grundsätzlich möglich. Die hohen datenschutzrechtlichen Maßstäbe für öffentlich-rechtliche Angebote können aber regelmäßig am besten durch die Rundfunkanstalt selbst realisiert und kontrolliert werden.

Sofern möglich, sollten die jeweiligen Nutzerdaten daher in der Rundfunkanstalt verarbeitet und gespeichert werden (z.B. Inhouse-Programmierung und dem Hosten der App auf anstaltseigenen Servern). Eine Durchführung durch externe Dritte sollte gegenüber einer anstaltsinternen Lösung nur nach Abwägung aller relevanten Aspekte bevorzugt werden.

× Vor Auftragsvergabe: Sind personenbezogene Daten betroffen?

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

× Bei Auftragsdatenverarbeitung: Beachtung der anstaltsinternen Regelwerke

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

× Hierauf ist besonders zu achten!

Einige Dienstleister arbeiten auch für private Anbieter und sind sich der besonders hohen datenschutzrechtlichen Standards für die Angebote der Rundfunkanstalten nicht immer bewusst. Oftmals ist für externe Dienstleister z.B. die Datenspeicherung außerhalb der EU üblich oder Dienstleister mit Sitz außerhalb der EU können auf Daten innerhalb der EU zugreifen. Für die Übermittlung/Verarbeitung von Daten in sog. Drittländer - d.h. Staaten außerhalb der EU - gelten besonders hohe Zulässigkeitsanforderungen; zudem sind zusätzliche datenschutzrechtliche Absicherungen erforderlich.

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

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

× Information über Verarbeitung von Nutzerdaten durch Dritte

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

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

CHATS, FOREN, GÄSTEBÜCHER, KOMMENTARFUNKTIONEN

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

Was sagt der Datenschutz?

Wer auf seiner Webseite Chats, Foren und andere interaktive Funktionen anbietet, verarbeitet Daten und Inhalte seiner Nutzer. In den meisten dieser Fälle müssen sich die Besucher registrieren oder zumindest eine E-Mail-Adresse angeben. Dadurch entsteht ein datenschutzrechtlich relevanter „Personenbezug". Interaktive Tools können aber auch so eingerichtet werden, dass jeder Besucher einen Beitrag ohne weitere Angaben veröffentlichen kann. Dabei ist aber zu bedenken, dass auch der Inhalt eines (vermeintlich) anonymen Beitrags einen Personenbezug im rechtlichen Sinne aufweisen kann. Rechtlich macht es daher fast keinen Unterschied, ob Nutzer sich registrieren müssen oder auch ohne weitere Angaben mitmachen können.

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

Checkliste

× Datenschutzrechtlich erforderliche Einwilligung des Nutzers

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

» die Beiträge der Nutzer selber,

» hinzu kommt in aller Regel ein Nutzername und oft auch ein Passwort sowie eine E-Mail-Adresse,

» auch bei einfachen Internetseiten fallen die Daten des HTTP-Requests an: IP-Adresse, Zeit des Zugriffs und andere Angaben.

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

Es ist nützlich, bei der Einwilligungserklärung die wichtigsten Informationen kompakt zusammenzufassen. Die Details können dann mit einem weiteren Klick - z.B. in der allgemeinen Datenschutzerklärung - verfügbar gemacht werden. Auch auf die Nutzungsbedingungen (s.u.) kann verlinkt werden.

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

× Nutzungsbedingungen und Netiquetten

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

Beispiele hierfür sind:

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

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

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

Die Netiquette bzw. die Nutzungsbedingungen sollten – wie die Einwilligung auch - durch den Nutzer aktiv bestätigt werden (z.B. via Checkbox). Die Nutzungsbedingungen können

einen eigenen Passus zum Datenschutz enthalten oder es kann auf die allgemeine Datenschutzerklärung des Onlineangebotes verlinkt werden.

× Löschung von persönlichen Nutzerdaten - Löschung von Inhalten

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

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

× Auf Datensicherheit achten

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

× Achtung bei der Verwendung von Nutzernamen

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

× Achtung bei Angeboten für Minderjährige

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

× Auf sonstige rechtliche Aspekte achten

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

COOKIES

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

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

» Session Cookies (temporäre Cookies)

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

» Permanente Cookies (dauerhaft gespeicherte Cookies)

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

Was sagt der Datenschutz?

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

× Unproblematisch: Für die Nutzung einer Seite unbedingt erforderliche Cookies

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

Regelmäßig handelt es sich hierbei um temporäre Cookies, die nach der Nutzung wieder gelöscht werden.

× Achtung bei optionalen Cookies für zusätzliche Zwecke

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

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

Checkliste

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

Angesichts der unklaren Rechtslage besteht derzeit eine Option darin, bis auf weiteres das „Opt-out"-Verfahren zu praktizieren und abzuwarten, wie sich die deutsche Rechtslage hier möglicherweise ändert. In diesem Fall hat die Rundfunkanstalt über den Einsatz von Cookies umfassend in der Datenschutzerklärung zu informieren und den Nutzer auf sein Widerspruchsrecht beim Einsatz von Cookies und bei der Bildung von Nutzungsprofilen hinzuweisen. Zudem ist dem Nutzer zu erklären, wie er das Setzen von Cookies verhindern bzw. diese durch Einstellungen in seinem Browser löschen kann.

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

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

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

ist zu protokollieren und vorzuhalten im Falle von Nachfragen.

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

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

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

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

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

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

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

× Achtung bei Angeboten für Minderjährige

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

DATENSCHUTZERKLÄRUNG

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

Was sagt der Datenschutz?

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

Eine Datenschutzerklärung ist strikt zu unterscheiden

» von einer datenschutzrechtlichen Einwilligung:

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

» vom Impressum einer Webseite:

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

Checkliste

× Form: Allgemein verständlich, leicht auffindbar und jederzeit abrufbar

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

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

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

× Inhalt: Was muss alles drin sein?

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

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

Informationen darüber, welche personenbezogenen Daten des Nutzers erfasst werden

» Bei Aufruf und Nutzung der Seite oder App

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

» Aufgrund der Anmeldung (Registrierung)

Name; Geschlecht; Geburtsdatum; Anschrift; Kontaktdaten (Mail, Telefonnummern), Fotos, Standortdaten o.ä.

» Aufgrund sonstiger Funktionen, insb. Anwendungen von externen Diensteanbietern

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

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

» Cookies und Plugins

Welche Cookies oder Plugins werden genutzt, welche Daten werden dabei wozu durch die Rundfunkanstalt oder Dritte genutzt?

» Tracking-Tools

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

» Zugriffsrechte (bei Apps)

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

» Eingaben des Nutzers

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

» Einwilligung

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

Information über Nutzerrechte

» Widerruf der Einwilligung

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

» Anonyme/pseudonyme Nutzung

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

» Widerspruchsrecht bei Cookies, pseudonymen Nutzungsprofilen

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

× Nennung eines Ansprechpartners

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

× Hinweis auf Drittplattformen, auf denen die Rundfunkanstalt präsent ist

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

DRITTPLATTFORMEN

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

Was sagt der Datenschutz?

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

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

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

Checkliste

× Überprüfung der Datenschutzrichtlinien / AGB der Drittplattform - Check des publizistischen Mehrwerts

Sofern die Rundfunkanstalt auf einer Drittplattform präsent sein will, sollten vorab die Datenschutzrichtlinien sowie die sonstigen AGB oder Nutzungsbedingungen des Drittanbieters

geprüft werden. Oftmals enthalten diese AGB für die Rundfunkanstalt problematische urheberrechtliche und sonstige Klauseln. Möglicherweise lässt sich der jeweilige Anbieter im Rahmen einer eigenen Vereinbarung mit allen Rundfunkanstalten zur Einhaltung der deutschen Standards bewegen.

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

× Datenschutzkonformes Verhalten der Rundfunkanstalt auf Drittplattformen

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

Dies bedeutet z.B., dass die Rundfunkanstalt die Nutzer nicht dazu einladen darf, sensible Informationen (z.B. im Rahmen von Upload-Aktionen) preiszugeben.

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

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

× Hinweis auf Nutzungsbedingungen der Drittplattform

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

Dem Nutzer sollte erklärt werden, dass die Datenverarbeitung durch die Betreiber der Drittplattformen außerhalb der Verantwortung der Rundfunkanstalten liegt. In diesem Kontext sollte - z.B. per Link - auch auf die allgemeinen Geschäftsbedingungen bzw. Datenschutzrichtlinien der jeweiligen Drittplattformen verwiesen werden.

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

EMBEDDING VON FREMDEN INHALTEN: PLUGINS, VIDEOS & CO

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

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

Was sagt der Datenschutz?

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

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

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

Checkliste

× Einbettung aus redaktionellen Gründen erforderlich?

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

× Gibt es datenschutzfreundliche Voreinstellungen?

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

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

× Einsatz der (modifizierten) Zwei-Klick-Lösung

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

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

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

Die Zwei-Klick-Lösung kann auch in einer modifizierten, nutzerfreundlicheren Version eingesetzt werden: Dabei wird der Nutzer pro Session beim Anklicken des ersten eingebetteten Inhalts auf einer Webseite auf einer Zwischenseite über die Datenverarbeitung durch die Drittanbieter aufgeklärt und hat die Wahl, auf weitere entsprechende Hinweise auf der Webseite

zu verzichten. Wenn er darauf verzichtet, wird die Zwischenseite bei nachfolgenden Einbettungen nicht jedes Mal wieder eingesetzt. Er hat damit die Option zur „generellen“ Freischaltung aller Drittanbieter-Inhalte auf der jeweiligen Webseite. Dieses Verfahren muss die Möglichkeit vorsehen, die pauschal erklärte Zustimmung jederzeit zu widerrufen.

× Shariff-Button für Social-Media-Plugins

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

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

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

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

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

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

× Achtung Auftragsdatenverarbeitung

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

Verarbeitet der Anbieter des Tools in diesem Zusammenhang Nutzerdaten, so tut er dies im Auftrag der Rundfunkanstalt; die Datenverarbeitung wird der Rundfunkanstalt zugerechnet. Es gelten hier die Hinweise zur ***Auftragsvergabe an Dritte***. Mit der Vereinbarung muss insbesondere sichergestellt werden, dass die Datenverarbeitung durch den Anbieter nur mit Wissen und Wollen der Nutzer erfolgen.

× Minderjährigen-Datenschutz

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

GEWINNSPIELE

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

Was sagt der Datenschutz?

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

Checkliste für Gewinnspiele im anstaltseigenen Onlineangebot

× Teilnahmebedingungen mit Informationen zum Datenschutz

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

× Zweckbindung und Datensparsamkeit

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

Die Pflichtfelder sind entsprechend kenntlich zu machen. Beispiele:

» Die Abfrage der Mailadresse ist ausreichend, wenn ein Versand des Preises (z.B. Tickets) online erfolgt und um eine Identifikationsmöglichkeit zu haben (z.B. um eine Mehrfachteilnahme zu verhindern).

» Die (zusätzliche) Telefonnummer ist zulässig, wenn eine telefonische Kontaktaufnahme (Rückruf) notwendig oder ein Telefongespräch on air geplant ist.

» Die Abfrage der Postadresse ist zulässig, wenn der Gewinn verschickt werden muss. Aber: In der Regel ist hier jedoch eine vorherige Kontaktaufnahme per Mail oder Telefon mit den Gewinnern möglich, so dass eine Adressangabe als Pflichtfeld bei allen Teilnehmern nicht immer erforderlich ist. Viele Nutzer sind außerdem nicht bereit, die Adresse als Pflichtfeld anzugeben.

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

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

× An die Löschung denken

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

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

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

× Minderjährigen-Datenschutz

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

× Achtung bei externen Dienstleistern

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

× Beachtung der sonstigen Vorgaben für Gewinnspiele

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

Checkliste für Gewinnspiele ausschließlich auf Drittplattformen:

× Verantwortlichkeit des Plattformanbieters

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

× Achtung bei Nutzerverarbeitung auch durch die Rundfunkanstalt

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

× Beachtung der sonstigen Vorgaben der Drittplattform

Es sind die sonstigen AGB/Richtlinien der jeweiligen Drittplattform zur Veranstaltung von Gewinnspielen zu beachten (vgl. z.B. Nutzungsbedingungen von Facebook ***www.facebook.com/page_guidelines.php***).

INSTANT MESSAGING

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

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

Was sagt der Datenschutz?

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

Checkliste

× Datensparsamkeit und Zweckbindung

Es gelten die allgemeinen Grundsätze (vgl. ***Datenschutz „Basics"***):

Es sollen so wenig Daten wie möglich erhoben werden; die Daten dürfen jenseits der journalistisch-redaktionellen Nutzung nur so lange gespeichert werden, wie es für diesen Zweck

erforderlich und notwendig ist. Sie dürfen nicht anderweitig verwendet werden. Danach sind die Daten zu löschen.

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

× Information in Datenschutzerklärung

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

× An die Löschung denken

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

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

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

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

× Lokale Datenspeicherung – keine automatische Synchronisation mit Dritten

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

× Achtung bei externen Dienstleistern

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

× Minderjährigen-Datenschutz

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

MAILKONTAKT, KONTAKTFORMULAR, NEWSLETTER

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

Was sagt der Datenschutz?

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

Checkliste

× Zweckbindung und Datensparsamkeit

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

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

× Besonderheiten beim Newsletter

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

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

» In jedem Newsletter muss der Nutzer deutlich sichtbar darauf hingewiesen werden, dass er den Newsletter jederzeit abbestellen kann. Hierzu ist ein Link in die Newsletter-Mail zu setzen.

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

× Informationen in der Datenschutzerklärung

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

× An die Löschung denken

Bei allen Kontaktformen muss sich die Redaktion darüber klar sein, wie lange welche Nutzerdaten warum aufbewahrt werden. Dazu muss man trennen, ob die personenbezogenen Daten - z.B. auch die eingesandten Fotos, „Geschichten" usw. - der Nutzer journalistisch-redaktionell genutzt werden (sollen) und eine Archivierung erfolgen soll oder nicht. Statistiken über Nutzer können anonym geführt werden.

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

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

× Datensicherheit - verschlüsselte Übertragung

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

ist.

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

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

× Minderjährigen-Datenschutz

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

× Achtung bei externen Dienstleistern

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

MINDERJÄHRIGEN-DATENSCHUTZ

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

Was sagt der Datenschutz?

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

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

Checkliste

× Vorab: Für welche Altersgruppe ist das Angebot gedacht?

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

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

Jugendliche ab 16 Jahren können in dieser Hinsicht wie Erwachsene behandelt werden. Für sie gelten keine Besonderheiten. Sie können ohne Mitwirkung der Eltern in eine Datenverarbeitung

einwilligen; ebenso können sie ihre Einwilligung auch jederzeit selbst widerrufen. Im Übrigen gelten sämtliche datenschutzrechtlichen Vorgaben und Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung usw. – vgl. ***Datenschutz „Basics"***).

× Einzelabwägung bei Jugendlichen von 13 bis 16 Jahren

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

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

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

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

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit usw. – vgl. ***Datenschutz „Basics"***).

× Achtung bei Kinder unter 13 Jahren: Einwilligung der Eltern erforderlich

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

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

Im Übrigen gelten die üblichen datenschutzrechtlichen Grundsätze (Datensparsamkeit, Zweckbindung, Transparenz, Löschung, Datensicherheit usw. – vgl. ***Datenschutz „Basics"***).

× Absolutes Muss: Kinderfreundliche Datenschutzerklärung

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

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

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

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

× Abstimmung mit dem Datenschutzbeauftragten

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

× Förderung der Medienkompetenz und Einsichtsfähigkeiten der Kinder und Jugendlichen

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

PERSONALISIERUNG

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

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

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

Was sagt der Datenschutz?

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

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

Checkliste

× Personalisierung durch persönliches Nutzerkonto

Personalisierung kann dadurch erreicht werden, dass der Nutzer sich freiwillig für ein eigenes Konto mit persönlichen Daten, Vorlieben und Interessen registriert. Der Nutzer muss sich hier

über ein eigenes Login anmelden und kann sein Konto einsehen und selbst verwalten. Auf diese Weise bekommt er nur für ihn zugeschnittene Inhalte angeboten, die er auf sämtlichen Endgeräten nutzen kann. In diesem Fall gelten die bekannten Datenschutzprinzipien (siehe *Datenschutz „Basics“*):

» Einwilligung

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

» Datensparsamkeit, Zweckbindung, Löschung, Datensicherheit

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

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

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

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

× Personalisierung über Pseudonymisierung/Anonymisierung

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

In diesem Fall ist auf folgendes zu achten:

» Wirksame Pseudonymisierung/Anonymisierung

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

» Möglichkeit des Widerspruchs bei Bildung pseudonymer Nutzerprofile

Sofern zum Zweck der Personalisierung pseudonyme Nutzerprofile gebildet werden, muss der Nutzer die Möglichkeit bekommen, der Bildung von Nutzerprofilen zu widersprechen (siehe hierzu

die Hinweise zur ***Web-Analyse***).

× Immer: Umfassende Informationen in der Datenschutzerklärung

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

× Minderjährigen-Datenschutz

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

SOCIAL LOGIN

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

Was sagt der Datenschutz?

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

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

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

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

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

Checkliste

× Information und Einwilligung unmittelbar beim Social Login

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

× Hinweis zum Social Login in eigener Datenschutzerklärung

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

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

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

× Alternative Registrierungsmöglichkeit

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

STANDORTDATEN

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

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

Was sagt der Datenschutz?

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

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

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

Checkliste

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

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

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

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

× Informationen zur Erhebung der Standortdaten und zur Aktivierung / Deaktivierung

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

× Datensparsamkeit: Erhebung und Nutzung nur der notwendigen Daten

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

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

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

× Sofern möglich: „Verwaschung“ des Standorts

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

× Wichtige Hinweise für die Löschung der Dienste

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

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

VOTINGS

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

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

Was sagt der Datenschutz?

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

Checkliste für Votings im anstaltseigenen Angebot

× Zweckbindung und Datensparsamkeit

Es sind so wenig Nutzerdaten wie möglich zu erheben: Zulässig sind nur die Daten, die für die Durchführung des Votings unbedingt notwendig sind (kein „nice to have“). Die erhobenen Daten dürfen nur so lange gespeichert werden, wie es für die Durchführung des Votings erforderlich ist. Sie dürfen für keine anderen Zwecke verwendet werden.

× Informationen in der Datenschutzerklärung

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

× Absicherung gegen Manipulation

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

× An die Löschung denken

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

× Achtung bei externen Dienstleistern

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

× Verknüpfung mit Gewinnspiel

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

× Verschlüsselung

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

× Minderjährigen-Datenschutz

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

Checkliste für Votings ausschließlich auf Drittplattformen

× Verantwortlichkeit des Plattformanbieters

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

× Achtung bei Nutzerverarbeitung auch durch die Rundfunkanstalt

Sobald die Nutzerdaten anlässlich des Votings auch in der Rundfunkanstalt verarbeitet werden, gelten die o.g. Vorgaben.

× Beachtung der sonstigen Vorgaben der Drittplattform

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

WEB-ANALYSE

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

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

Was sagt der Datenschutz?

Bei Web-Analyseverfahren können personenbezogene Daten anfallen, so z.B. auch die

IP-Adresse des Nutzers. Hierfür ist grundsätzlich die Einwilligung des Nutzers erforderlich.

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

Checkliste

× Personenbezogene Nutzungsprofile nur mit Einwilligung

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

× Vorsicht bei IP-Adressen

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

× Pseudonyme Nutzerprofile ohne Einwilligung zulässig

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

» Pseudonyme:

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

» Widerspruchsrecht:

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

» Strikte Datentrennung:

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

× Anonyme Nutzungsprofile unterliegen nicht dem Datenschutz

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

× Pflicht zur Information in der Datenschutzerklärung

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

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

× Achtung beim Einsatz von Cookies

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

× Achtung: Auftragsdatenverarbeitung!

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

» Herausgeber: Arbeitskreis der Datenschutzbeauftragten von ARD, ZDF und Deutschlandradio

» Redaktion: Barbara Nickel, Bayerischer Rundfunk

» Design: Henrik Ullmann, Bayerischer Rundfunk – Abt. Multimedia Design

» Stand: September 2016