

Datenschutz und Datensicherheit bei Social-Media-Angeboten der Rundfunkanstalten - Leitfaden -

A. Vorbemerkungen

Mit diesem Leitfaden wird der Leitfaden des AK DSB zu Datenschutz und Datensicherheit in Sozialen Netzwerken vom Mai 2009 aktualisiert und ergänzt.

Soziale Medienangebote (Social Media) dienen dazu, sich mithilfe digitaler Medien und Technologien untereinander auszutauschen. Zu diesem Zweck werden persönliche Daten - auch digitale Fotos und Videos - in aller Welt mehr oder weniger verfügbar gemacht. Zu Social Media gehören interaktive Angebote und Dienste, wie u.a. Chats, Foren Blogs und Soziale Netzwerke.

Social-Media-Angebote dominieren zunehmend das Mediennutzungsverhalten in bestimmten Zielgruppen. Daher verwenden auch die öffentlich-rechtlichen Rundfunkanstalten solche Angebote und sind auch selbst Betreiber von Sozialen Netzwerken z.B. durch die Hörfunkwellen MeinFritz.de vom rbb, mySPUTNIK.de vom MDR und myYOU-FM.de vom hr. Diese Sozialen Netzwerke ermöglichen es den Nutzern, mit Gleichgesinnten in Kontakt zu treten, sich an dem öffentlichen Meinungsbildungsprozess zu beteiligen und beispielsweise eigene Musik mittels eines entsprechenden Videoclips zu veröffentlichen. Um zusätzliche Zielgruppen zu erreichen, bieten die öffentlich-rechtlichen Rundfunkanstalten inzwischen ihre Angebote auch auf den Plattformen anderer Anbieter - insbesondere auf Facebook und YouTube - an. Diese Entwicklung ist aus Sicht des Datenschutzes kritisch zu betrachten, da die meisten Social Media Plattformen Dritter momentan weder den deutschen Datenschutzgesetzen noch den Standards der ARD-Datenschutzbestimmungen genügen.

Aus diesem Grund kommt der Aufklärung der Nutzer über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten eine besondere Bedeutung zu. Das betrifft auch die Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Besondere Schwerpunkte der Aufklärung müssen auch der Umgang mit den Daten Dritter und der Jugendschutz, der u. a. bei den Angeboten des Kinderkanals von ARD und ZDF eine große Rolle spielt, bilden. Der Vollständigkeit halber sei darauf hingewiesen, dass über die datenschutz- und persönlichkeitsrechtlichen Aspekte hinaus weitere Themen wie z. B. das Urheber-, das Kennzeichen- und Markenrecht sowie das Strafrecht zu beachten sind.

Nachfolgend werden die wesentlichen Anforderungen zu Datenschutz und Datensicherheit bei Social-Media-Angeboten der Rundfunkanstalten dargestellt.

Dieser Leitfaden richtet sich an alle Mitarbeiterinnen und Mitarbeiter, die Social Media im Auftrag der Rundfunkanstalten redaktionell einsetzen bzw. die technischen Voraussetzungen dafür schaffen. Der Leitfaden soll eine erste Orientierung bieten. Er kann den Informationsaustausch zwischen den verantwortlichen Mitarbeiterinnen und Mitarbeitern und den Rundfunkdatenschutzbeauftragten zu Einzelfragen nicht ersetzen.

B. Datenschutz - was ist ganz generell zu beachten?

Datenschutz hat das Ziel, jeden einzelnen Menschen vor den Gefahren beim Umgang mit persönlichen Daten zu schützen. Datenschutz ist daher immer dann zu beachten, wenn personenbezogene Daten abgefragt und verwendet werden.

Unter personenbezogenen Daten versteht man alle Daten, die dazu genutzt werden können, die Identität des Users offen zu legen, wie z. B. richtiger Name, Anschrift, Telefonnummer, E-Mail- und IP-Adresse sowie weitere Informationen z. B. über das Nutzungsverhalten, soweit sie dem Nutzer zugeordnet werden können. Besonders sensible persönliche Daten sind z.B. Angaben über die ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben sowie Daten über Straftaten und Minderjährigendaten.

Für ein datenschutzkonformes Onlineangebot der Rundfunkanstalten gilt ganz generell Folgendes:

- Eine Erhebung, Speicherung und Nutzung der personenbezogenen Daten eines Nutzers darf grundsätzlich immer nur zu einem bestimmten, jeweils angegebenen Zweck erfolgen. Eine Verwendung der Daten für andere Zwecke ohne Wissen und Einverständnis des Nutzers ist unzulässig. Name, Anschrift, Mailadresse oder Telefonnummer u.ä. eines Nutzers dürfen nie pauschal abgefragt und gespeichert werden (Grundsatz der Zweckbindung).
- Der Nutzer muss genau wissen, für wen/was er welche Daten zur Verfügung stellt (Transparenzgebot) und er muss hierzu seine Einwilligung erklären. Wenn also in den einzelnen Fällen (z.B. bei Gewinnspielen, beim Versand von Newslettern, bei der Anmeldung für Communities etc.) personenbezogene Informationen eines Nutzers benötigt und gespeichert werden, muss er ausdrücklich und in transparenter Weise auf diesen Sachverhalt aufmerksam gemacht werden. Aus verschiedenen Quellen/Anlässen stammende personenbezogene Daten dürfen nicht zu einem Profil zusammengeführt werden, soweit nicht hierzu die gesondert einzuholende Einwilligung des Nutzers erteilt wurde. Nutzer müssen ein Angebot nutzen können, ohne zuvor einer Profilbildung zustimmen zu müssen.

- Sollen besonders sensible persönliche Daten erhoben, verarbeitet oder genutzt werden, so ist der Nutzer darüber im Zuge seiner Einwilligung gesondert zu unterrichten.
- Es sollen immer so wenige Pflicht-Daten wie möglich, also nur solche Daten, die wirklich erforderlich sind (Prinzip der Datensparsamkeit), abgefragt werden. Beispiel für einen begründeten Ausnahmefall ist die Abfrage von E-Mail-Adressen bei Kommentarfunktionen (nicht öffentlich sichtbar). In der Praxis hat sich gezeigt, dass diese Vorgabe, wenngleich sie de facto keine persönliche Identifizierung ermöglicht, positive Auswirkungen auf das Niveau der Kommentare und den Umgang der Nutzer untereinander hat.
- Der Nutzer hat das Recht, seine erteilte Einwilligung zur Datenspeicherung mit Wirkung für die Zukunft jederzeit zu widerrufen. Auf dieses Recht muss er ausdrücklich hingewiesen werden.
- Sobald die personenbezogenen Daten nicht mehr zu dem ursprünglich angegebenen Zweck benötigt werden, müssen sie gelöscht bzw. anonymisiert werden. Das gleiche gilt im Falle des Widerrufs einer Einwilligungserklärung in die Datenverarbeitung durch den Nutzer.
- Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist durch geeignete technische und organisatorische Maßnahmen so zu gestalten, dass die Daten vor Fehlern, Missbrauch und Zerstörung geschützt sind (Maßnahmen zur Datensicherheit).
- Der Kontaktweg zur Nutzerbetreuung sollte, ebenso wie das Impressum und der Verweis auf die Beschwerde-/Widerrufsmöglichkeit, für die Nutzer leicht auffindbar sein.

C. Einzelne Datenschutzmaßnahmen auf den Webseiten der Rundfunkanstalten

I. Schulung von Medienkompetenz

Die Angebote der Rundfunkanstalten sollen die Nutzer über die spezielle Problematik von Privatsphäre in Social-Media-Angeboten aufklären. Hierfür sollten zielgruppengeeignete Formen gefunden werden, so zum Beispiel eine Erläuterung der Risiken in Videos.

II. Datenschutzkonforme Gestaltung

1. Beschränkung der Pflichtangaben auf das notwendige Minimum

Der Umfang der von den Nutzern bei der Anmeldung zu Social Media (Registrierung) abzugebenden persönlichen Pflichtangaben ist auf das für die technische Realisierung oder die Erfüllung rechtlicher Auflagen notwendige Minimum zu beschränken (Prinzip der Datensparsamkeit). Dabei hilft die Kontrollfrage: Wozu brauchen wir die Angaben?

Eine anonyme Nutzungsmöglichkeit ist vorab zu prüfen. Eine pseudonyme Nutzung muss möglich sein. Dabei ist der Benutzername nicht mit dem echten Namen

identisch, sondern ein frei wählbarer Name. Mit diesem Benutzernamen ist der Teilnehmer in dem Social Media-Angebot sichtbar. Es kann aber nicht direkt auf die Person geschlossen werden.

2. „Datenschutzerklärung“/ Unterrichtung

Die Rundfunkanstalt hat in ihrem Onlineangebot die Nutzer in einer Datenschutzerklärung über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten zu informieren. Die Unterrichtungspflicht bezieht sich sowohl auf die Inhaltsdaten (siehe Glossar im Anhang) als auch auf die Bestands- und Nutzungsdaten. Je mehr Daten von den Nutzern erhoben werden und je sensibler die Daten sind, desto ausführlicher muss die Unterrichtung sein. Zudem sollte der Nutzer auf das Einwilligungserfordernis und die Möglichkeit des Widerrufs hingewiesen werden. Des Weiteren sollte der Nutzer ausdrücklich auf die Möglichkeit der pseudonymen Nutzung hingewiesen werden. Falls Cookies verwendet werden, ist auch hierüber genau zu informieren (siehe hierzu 12.). Schließlich sollte auch ein Kontakt für datenschutzrechtliche Anfragen und Beschwerden (z.B. der anstaltseigene Datenschutzbeauftragte) genannt werden.

Die Datenschutzerklärung sollte in allgemein verständlicher Form formuliert sein und muss leicht auffindbar und jederzeit abrufbar sein. Eine Datenschutzerklärung muss grundsätzlich für das gesamte Onlineangebot einer Rundfunkanstalt formuliert werden. Für Internetangebote, die sich an Minderjährige richten, ist zusätzlich eine verständliche Form für Kinder wünschenswert (vgl. III).

Sofern es im Rahmen dieses Onlineangebots Social-Media-Angebote gibt, bieten sich entweder eigene Unterrichtungen (z.B. über einen eigenen Link) zusammen mit den Nutzungsbedingungen speziell zu den Social-Media-Angeboten an. Andernfalls sollten in der allgemeinen Datenschutzerklärung eigene Punkte zu „Social Media“ - insbesondere zu den Sozialen Netzwerken - mit ausführlichen Informationen enthalten sein.

3. „Aktive“ Einwilligung in die Verarbeitung der personenbezogenen Daten

Für die dauerhafte Speicherung von personenbezogenen Daten für einen bestimmten Zweck ist eine aktive Einwilligung des informierten Nutzers erforderlich. Die Einwilligung muss eindeutig und bewusst erfolgen.

Erreichen lässt sich diese Anforderung z. B., indem der Nutzer ein bestimmtes Feld im Anschluss an die Einwilligungserklärung ankreuzen muss (Checkbox), die ihm anschließend auch dargestellt wird, bevor er die angekreuzte Einwilligungserklärung an die Rundfunkanstalt durch das Anklicken eines Bestätigungsfeldes übersendet. Geeignet ist auch ein Verfahren, bei dem die Rundfunkanstalt dem Nutzer die Einwilligungserklärung noch einmal per E-Mail übersendet und sich den Empfang durch das Anklicken eines in der E-Mail abgegebenen Aktivierungslinks bestätigen lässt (sog. double opt-in-Verfahren).

Die Einwilligung muss dabei dort eingeholt werden, wo die Daten erhoben oder weitergegeben werden und gilt nur für den beschriebenen Zweck. Die Einholung

einer Einwilligung zu Datenverarbeitungen für sämtliche Social Media-Angebote ist nur dann möglich, wenn der Nutzer hierüber ausdrücklich informiert wird und außerdem weiterhin auch die „einfache“ Anmeldung zu einem speziellen Social-Media-Angebot und die dann selbst ausgewählte Teilnahme an den dort angebotenen Einzelaktionen möglich bleibt.

Die Einwilligung muss protokolliert werden und jederzeit für den Nutzer abrufbar sein. Es ist ausreichend, wenn die Einwilligung jeweils auf Anfrage zugänglich gemacht wird.

Eine gesonderte Protokollierung kann entfallen, wenn der Zugriff auf die Angebote technisch an eine Einwilligungserklärung gebunden wird, also kein Anmeldeprozess ohne Zustimmung zu den Erklärungen möglich ist. Bei diesem Modell muss die Zustimmung bei Änderung der Bestimmungen zwingend neu eingeholt werden.

Generell sollte im Fall der Änderung der Datenschutzbestimmungen jeweils eine neue Einwilligungserklärung der Nutzer eingeholt werden und auf standardmäßige Änderungsklauseln wie: „Das Recht zu jederzeitigen Änderung an diesen Datenschutzbestimmungen wird vorbehalten...“ verzichtet werden.

4. Einfache Möglichkeit des Widerrufs der Einwilligung

Die Einwilligung muss jederzeit in einfacher Art und Weise vom Nutzer widerrufbar sein. Der Nutzer muss jedenfalls in der Datenschutzerklärung über sein Widerrufsrecht informiert werden.

5. Aktive Freigabe der Daten durch den Nutzer

Die Daten, die der Nutzer im Rahmen der Anmeldung als Information auf seinem Profil angibt, dürfen zunächst bis auf den Benutzernamen nicht für andere Nutzer sichtbar sein. Der Nutzer muss selbst die Möglichkeit haben und entscheiden können, ob und welche Informationen er für andere Nutzer der Social-Media-Angebote sichtbar macht. Im Rahmen der Einstellungen ist ein differenziertes Berechtigungskonzept nötig (s. 6.).

6. Differenziertes Berechtigungskonzept bei Sozialen Netzwerken

Für ein Soziales Netzwerk muss ein differenziertes Berechtigungskonzept festgelegt und umgesetzt werden. Der Nutzer muss dabei selber die Regeln festsetzen können,

- welche seiner Datenobjekte (Fotos, Freunde, Gästebuch, persönliche Daten)
- von welcher Gruppe der Zugreifenden - z. B. Freunde - Mitglieder des Sozialen Netzwerks - allgemeine Öffentlichkeit (d.h. auch von Nichtmitgliedern des Sozialen Netzwerks),
- mit welchen Rechten (z.B.: lesen, schreiben, ändern) versehen wird.

Mit einer Art „Ampelsystem“ sollte den Nutzern deutlich angezeigt werden, welcher Kreis auf die jeweiligen Daten aktuell zugreifen kann. Die Ampelmetapher kann dem

Nutzer bei der Erstellung sowie bei der späteren Ansicht den Berechtigungsstatus seiner Inhalte visualisieren. Der Berechtigungsstatus sollte auch über diese Ampel änderbar sein.

Das Recht zur Selbstbestimmung und der Persönlichkeitsrechtsschutz dürfen nicht durch eine vorhandene Suchfunktion unterlaufen werden. Die Suchfunktion muss also die vom Profilinhaber eingerichteten Zugriffskontrollen berücksichtigen.

Bei der Möglichkeit des schreibenden Zugriffs (z.B. in Form eines Eintrags in das Gästebuch) muss dem Profilinhaber ein Vetorecht eingeräumt werden.

7. Profil-Besucher-Historie

Sofern in den Social-Media-Angeboten, insbesondere bei Sozialen Netzwerken, auch eine Protokollfunktion vorgesehen ist, mit der für die Mitglieder sichtbar ist, welcher Nutzer welches Profil besucht hat, sollte diese Funktion als Defaulteinstellung nicht aktiviert sein. Der Profilinhaber muss selbst entscheiden können, ob er diese Defaulteinstellung ändern will.

8. Begrenzung des Zugriffs auf Social Media von außen

Der Zugriff auf (sensible) personenbezogene Daten der Nutzer durch Nichtmitglieder insbesondere bei Sozialen Netzwerken, von außen, d.h. vom allgemein zugänglichen Teil des Internet auf ein solches Angebot (z. B. über Suchmaschinen) muss technisch ausgeschlossen sein. Auch der Export oder Download von persönlichen Daten, die Teil des Profils eines Nutzers sind, durch Dritte muss - sofern technisch möglich - ausgeschlossen sein.

Es muss sichergestellt sein, dass personenbezogene Daten durch Dritte (z. B. Besucher und Suchmaschinen) nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Dazu zählen auch Profilbilder in selbst betreuten Nutzerprofilen.

9. Daten Dritter

Der Nutzer muss möglichst in einem entsprechenden Textfeld, mindestens aber in den Nutzungsbedingungen, deutlich darauf hingewiesen werden, dass er bei den von ihm eingestellten Inhalten die Persönlichkeitsrechte Dritter zu beachten hat; insbesondere müssen die in seinen Bildern, Videos etc. abgebildeten Personen ihre Einwilligung - soweit nach der Rechtslage eine solche nicht entbehrlich ist - zur Veröffentlichung erteilt haben. Für den Fall des widerrechtlichen Einstellens von Daten Dritter sollte sich die Rundfunkanstalt den sofortigen Ausschluss aus ihrem Angebot vorbehalten.

10. Aufgabe der Mitgliedschaft

Es muss eine unkomplizierte Möglichkeit für die Aufgabe der Mitgliedschaft eingerichtet werden. Diese Abmeldefunktion muss auf der Plattform selbst vorhanden

und einfach durchzuführen sein. Nicht ausreichend ist die Abmeldemöglichkeit per Email oder Brief an die Rundfunkanstalt.

11. Nach Aufgabe der Mitgliedschaft vollständige Löschung oder Anonymisierung der personenbezogenen Daten

Personenbezogene Daten des Nutzers müssen umgehend nach der Aufgabe einer Mitgliedschaft und der entsprechenden Abmeldung in einem technischen Vorgang automatisch gelöscht werden. Diese vollständige Löschung sollte auch die vom Anwender erzeugten Daten außerhalb des Profils erfassen.

Ist eine Löschung technisch nicht möglich, müssen die Daten in jedem Falle anonymisiert werden. Anonymisiert sind die Daten dann, wenn die personenbezogenen Daten derart verändert sind, dass die Informationen einer bestimmten oder bestimmbarer natürlichen Person nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft zugeordnet werden können.

12. Cookies

Die Zulässigkeit der Verwendung von Cookies im konkreten Einzelfall richtet sich nach den allgemeinen datenschutzrechtlichen Grundsätzen, wenn das Cookie personenbezogene Daten (z. B. die IP-Adresse) enthält.

Die Verwendung von Cookies als Nutzungsdaten ist gesetzlich zulässig und bedarf keiner gesonderten Einwilligung, sofern sie für die aktuelle Nutzung der Dienste erforderlich ist. Als Nutzungsdaten sind die Informationen zu betrachten, die während der Nutzung des Online-Angebots, also insbesondere der Interaktion mit dem Anbieter des Social Media Angebots, entstehen. Hierbei handelt es sich dann um ein temporäres Cookie (sog. „session cookie“), das nach der Nutzung wieder gelöscht wird.

Das Setzen sog. „permanenter“ Cookies (d.h. Cookies, die dauerhaft auf der Festplatte des PC abgelegt werden) mit personenbezogene Daten ist grundsätzlich nur mit Einwilligung des Nutzers zulässig. Eine Einwilligung ist dann nicht erforderlich, wenn mit Hilfe des Cookies anonymisierte oder pseudonymisierte Nutzerprofile für Zwecke der Marktforschung oder zur bedarfsgerechten Gestaltung des Dienstes gebildet werden. Der Bildung eines pseudonymisierten Nutzerprofils muss ein Nutzer jedoch jederzeit widersprechen können.

Unterrichtungspflicht bei Einsatz von Cookies

Der Nutzer muss über die Art, den Umfang und den Zweck des Einsatzes eines Cookies in allgemein verständlicher Form unterrichtet werden. Falls das Cookie die Erhebung oder Verwendung personenbezogener bzw. -beziehbarer Daten vorbereitet, hat die Information über den Einsatz eines Cookies „zu Beginn“ des Einsatzes zu erfolgen. Der Hinweis muss vor dem Einsatz, also vor dem „Ablegen“ des Cookie, gegeben werden. Praktisch muss der Hinweis so rechtzeitig erfolgen, dass der Betroffene die spätere Identifikation noch verhindern kann. Der Nutzer muss dabei klare und ausführliche Informationen über die Verwendung/den Zweck,

den Inhalt und das Verfallsdatum des Cookie erhalten und in die Lage versetzt werden, Permanent-Cookies auch ablehnen zu können (üblicherweise dadurch, dass der Nutzer darauf hingewiesen wird, dass er durch technische Maßnahmen/Veränderung der Browsereinstellung die Durchführung von Permanent-Cookies abwenden kann).

Die Nutzung des Angebots muss auch ohne Permanent-Cookie weiterhin möglich sein. Darüber und über die Tatsache, dass der Nutzer in diesem Fall mit Funktionseinschränkungen rechnen muss, ist er in der Datenschutzerklärung zu informieren. Nicht ausreichend ist der kommentarlose Verweis auf die Einstellung im Browser („Cookie akzeptieren“) oder die Zustimmung zu einer Anfrage ohne entsprechende Unterrichtung („xxx will ein Cookie installieren. Sind Sie damit einverstanden?“).

13. Speicherung der Protokolldaten

Es sind geeignete technische und organisatorische Maßnahmen zu treffen, um einen sicheren Betrieb und eine sichere Nutzung der Social Media und der gespeicherten persönlichen Daten zu gewährleisten (näheres dazu s. E). Die Protokolldaten der Nutzer, die bei der Nutzung der Social-Media-Angebote auf den Onlineseiten der Rundfunkanstalten anfallen (insbesondere die IP-Adresse), dürfen im Regelfall maximal 7 Tage gespeichert und ausschließlich für Zwecke der Datensicherheit verwendet werden. Anlassbezogen können die Daten mit Zustimmung der/des Datenschutzbeauftragten im Einzelfall bei Bedarf auch länger gespeichert werden. In Abstimmung mit der/dem Datenschutzbeauftragten ist eine strikte Regelung zur Zweckbindung, den Berechtigungen und dem Umgang mit diesen Daten in den einzelnen Häusern zu etablieren.

14. Widget

Grundsatz: Keine Verwendung von Widgets, die Daten der Nutzer verarbeiten

Unter Widgets werden Komponenten eines Fenstersystems verstanden. Es handelt sich um kleine Elemente auf dem Desktop. Sie können z.B. den Posteingang von E-Mail-Konten, die Uhrzeit, aktuelle Verkehrs- und Wettermeldungen anzeigen oder aktualisierbare Nachrichtenschlagzeilen. Grundlage eines Widgets ist eine sog. Widget-Engine, eine Software, die die Voraussetzung für die Nutzung von Widgets bildet. Widget-Engines werden z.B. von Apple, Google, Microsoft angeboten.

Wenn der Dienstleister personenbezogene Daten wie die IP-Adresse der Nutzer verarbeitet, ist dies datenschutzrechtlich relevant und berührt auch die Informationsfreiheit der „getrackten“ Nutzer. Daher ist diese Frage, ob personenbezogene Daten verarbeitet werden, unbedingt **vor** dem Einsatz eines Widgets zu klären.

15. Aktuelles Beispiel: Nutzung von Facebook Social Plugins („Gefällt-mir“-Buttons)

Facebook gestattet anderen Webseitenbetreibern auf den eigenen Seiten "Gefällt mir" Buttons und andere Elemente des Facebook-Netzwerkes einzubauen, sog. Social Plugins. Facebook kann auch ohne Betätigung des "Gefällt mir" Buttons Nutzer bereits mit dem Aufruf der Seite, die das Plugin enthält (und nicht erst mit

dem Anklicken des Social Plugins), identifizieren: Der Browser stellt nämlich gleichzeitig auch eine Verbindung zu den Servern von Facebook her. Der Inhalt des Plugins (das u.a. die IP-Adresse enthält) wird von Facebook direkt an den Browser des Nutzers übermittelt und von diesem in die Webseite eingebunden. Facebook erhält so nicht nur einen Social Graph, wem was gefällt, sondern auch Informationen über einen Teil der Seiten, die Facebook Nutzer im Netz besucht haben. Je mehr Seiten (auch der Rundfunkanstalten) die Social Plugins nutzen, desto umfassender kann Facebook das Surfverhalten von Nutzern erfassen.

Dies ist datenschutzrechtlich unzulässig, da letztlich die IP-Adresse eines Nutzers ohne Vorwarnung, ohne Wissen und möglicherweise gegen seinen Willen von dem eigentlichen Betreiber der Seite auch an Facebook geliefert wird - und das nur, weil der Nutzer auf eine bestimmte Seite geht, auf der dieses Plugin eingebaut ist. Dies verstößt gegen die Datenschutzbestimmungen der Rundfunkanstalten.

Daher wird von einem Einbau der Social Plugins von Facebook und anderer Widgets, die personenbezogenen Daten verarbeiten, auf den Seiten der Rundfunkanstalten grundsätzlich abgeraten.

16. Ausnahmsweiser Einbau von Widgets oder Social Plugins

Möchte eine Redaktion trotz der datenschutzrechtlichen Problematik ausnahmsweise ein Widget, mit dem personenbezogene Daten verarbeitet werden, nutzen, sollte ein klarer redaktioneller Nutzen für die Rundfunkanstalt und die Nutzer ersichtlich sein.

In diesem Fall müssen die Rundfunkanstalten außerdem als Webseitenbetreiber die Verwendung von Widgets in ihren Datenschutzhinweisen erläutern.

Außerdem muss den Nutzern die Möglichkeit eröffnet werden, das entsprechende Angebot auch ohne Widgets zu nutzen.

Eine etwaige ungewollte Übermittlung von Daten ist durch ein vorgeschaltetes Element zu unterbinden, das den Nutzer in verständlicher Form darüber informiert, dass er beim Anklicken Daten vom jeweiligen Anbieter lädt und ihm die Wahlmöglichkeit lässt, die Seite mit dem Widget aufzurufen (2-Klick-Lösung).

17. Technische Aspekte

Medienbrüche (= Wechsel von einer Plattform oder einem Prozess auf eine/n andere/n mit der Gefahr der Informationsverfälschung) sollten weitestgehend verhindert werden, um eine höhere Revisionssicherheit zu gewährleisten.

Bei allen Angeboten sollte die nachträgliche Löschung und/oder Anonymisierung durch den Nutzer von vorne herein bei der Konzeption mit eingeplant werden.

III. Besonderheiten bei Angeboten für Minderjährige

1. Verfahren

An Minderjährige gerichtete Social-Media-Angebote sollen nur nach einer Vorab-Bewertung durch die/den zuständigen Datenschutzbeauftragten produktiv genommen werden. Eine Vorab-Bewertung soll auch bei einer wesentlichen inhaltlichen oder gestalterischen (prozessualen) Veränderung/Neuausrichtung bestehender Angebote erfolgen.

2. Inhaltliche Ausgestaltung

An Minderjährige gerichtete Angebote sollen hinsichtlich des Datenschutzes und der Datensicherheit den höchsten Maßstäben entsprechen, die für an Erwachsene adressierte Angebote derselben Rundfunkanstalt gelten.

Im Übrigen soll hinsichtlich der Anforderungen zu Datenschutz und Datensicherheit differenziert werden zwischen Angeboten

- für Kinder, bei denen es sich um „Internet-Einsteiger“ handelt (etwa bis zum Alter von 13 Jahren) (Gruppe 1) und
- für Minderjährige, die erwartbar bereits Internet-Erfahrung besitzen und dazu tendieren, auch andere Online-Angebote mit geringerem Schutz-Niveau (kommerzielle Communities, usw.) zu nutzen (etwa ab dem Alter von 14 Jahren) (Gruppe 2).

Bei Angeboten für die Gruppe 1 sollte eine Verknüpfung mit Drittangeboten nicht stattfinden. Die Erläuterungen zum Datenschutz sollten sowohl kindgerecht, als auch erwachsenengerecht erfolgen. Das Ziel ist, Kinder an das Thema Datenschutz heranzuführen und Eltern zu informieren. In Angeboten für Gruppe 2 sollten Verknüpfungen mit Drittangeboten unter den in D. genannten Voraussetzungen möglich sein, mit der Zielsetzung, einen verantwortungsvollen und aufgeklärten Umgang auch mit solchen Online-Angeboten zu vermitteln.

3. Einwilligung

Sofern Minderjährige unter 14 Jahren bei einem von der ARD betriebenen Sozialen Netzwerk Mitglied werden dürfen - das zulässige Alter sollte in den Nutzungsbedingungen geregelt sein -, muss grundsätzlich die schriftliche Einwilligung der Erziehungsberechtigten zur Speicherung und Nutzung personenbezogener Daten des Minderjährigen ergänzend eingeholt werden.

Geeignet ist - in erster Linie bei Minderjährigen ab 14 Jahren - auch ein double opt-in-Verfahren, bei dem die Rundfunkanstalt dem Minderjährigen an die von ihm anzugebende E-Mail-Adresse seiner Eltern/Erziehungsberechtigten die Einwilligungserklärung noch einmal per E-Mail übersendet und sich den Empfang durch die

Eltern/Erziehungsberechtigten durch das Anklicken eines in der E-Mail abgegebenen Aktivierungslinks bestätigen lässt.

Ein Absehen von dem Erfordernis der Einwilligung der Eltern ist nur im begründeten Ausnahmefall und nach Rücksprache mit der/dem Datenschutzbeauftragten möglich.

D. Social Media Plattformen Dritter

Im Rahmen des Programmauftrags der Rundfunkanstalten kommen auch Kooperationen mit bestehenden, auch kommerziellen Anbietern von Social Media in Betracht. Die Rundfunkanstalten wirken darauf hin, dass bei derartigen Kooperationen die vorstehend beschriebenen datenschutzrechtlichen Anforderungen berücksichtigt werden.

I. Anforderungen an Anbieter von Social Media

Sollten die Nutzungsbedingungen des Drittplattformbetreiber *nicht* den Datenschutzstandards der Rundfunkanstalten entsprechen, so haben die Rundfunkanstalten bei Interesse an einer Kooperation darauf hinzuwirken, dass im Rahmen der Zusammenarbeit die Einhaltung der datenschutz- und datensicherheitsrechtlichen Vorgaben der Landesrundfunkanstalten auf dieser Drittplattform sichergestellt ist.

Es muss insbesondere ausgeschlossen sein, dass das Nutzungsverhalten bezogen auf Inhalte der Rundfunkanstalten auf Plattformen Dritter durch diese Plattformen personenbezogen ausgewertet wird, soweit Nutzer dem nicht ausdrücklich zustimmen. Die Drittplattformen dürfen außerdem in keinem Fall Daten über die Nutzung und das Nutzungsverhalten ihrer User an Dritte weitergeben.

Um eine Möglichkeit zur Durchsetzung dieser Position, insbesondere auch gegenüber den marktstarken Anbietern zu haben, empfiehlt es sich, seitens der ARD insgesamt Rahmenbedingungen für die Präsenz eigener Angebote auf fremden Plattformen mit den jeweiligen Plattformbetreibern zu vereinbaren. Die zuständigen Datenschutzbeauftragten sollten bei entsprechenden Verhandlungen einbezogen werden.

Bei der Bewertung, inwieweit sich Anbieter von Social Media datenschutzkonform verhalten bzw. in Vereinbarungen auf Datenschutzkonformität verpflichtet werden können, ist - abgesehen vom nationalen Rechtsrahmen - ein Blick auf die Befassung der sog. Artikel 29 EU-Datenschutzgruppe hilfreich (vgl. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_de.pdf, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2010_05_12_letter_art29wp_signatories_safer_social_networking_principles_en.pdf).

Kernpunkte für die Datenschutzkonformität sind danach:

SNS (= Social Network Services) erkennen die Anwendbarkeit der EG-Datenschutzrichtlinie auf die Verarbeitung personenbezogener Daten durch SNS auch dann an, wenn diese ihren Hauptsitz außerhalb des Europäischen Wirtschaftsraums haben. Die Anbieter sozialer Netzwerkdienste gelten als für die Verarbeitung Verantwortliche im Sinne der EG-Datenschutzrichtlinie.

Die Nutzer gelten in Bezug auf die Verarbeitung ihrer personenbezogenen Daten durch die SNS als betroffene Personen. Die Verarbeitung personenbezogener Daten durch die Nutzer selbst fällt in den meisten Fällen unter die Ausnahmeklausel für Privathaushalte.

SNS sollten ihre Nutzer über ihre Identität aufklären und umfassende und eindeutige Informationen über ihre Zielsetzungen sowie über die verschiedenen Möglichkeiten vorlegen, wie sie die personenbezogenen Daten verarbeiten wollen. Werbemaßnahmen müssen im Einklang mit den einschlägigen Bestimmungen der EG-Datenschutzrichtlinie und der EG-Datenschutzrichtlinie für elektronische Kommunikation stehen.

SNS sollten datenschutzfreundliche Standardeinstellungen anbieten. SNS sollten den Nutzern ausreichende Informationen und geeignete Warnhinweise zu den Risiken für den Schutz ihrer Privatsphäre an die Hand geben, die mit dem Hochladen von personenbezogenen Daten ins soziale Netzwerkprofil verbunden sind. SNS müssen sich festlegen, wie lange die Vorratsspeicherung von Daten inaktiver Nutzer im Höchstfall zulässig ist. Aufgegebene Nutzerprofile sind zu löschen.

SNS sollten besonders auf den Schutz Minderjähriger achten. Den Nutzern sollte es im Allgemeinen gestattet sein, ein Pseudonym anzunehmen.

Die Nutzer sollten vom SNS darauf hingewiesen werden, dass Bilder oder Informationen über dritte Personen nur mit der Einwilligung der betroffenen Person ins soziale Netzwerkprofil eingestellt werden sollten.

Die Homepage des SNS sollte zumindest einen Link zu einer Beschwerdestelle aufweisen, die sich mit den Datenschutzfragen der Mitglieder wie auch der Nichtmitglieder befasst.

II. Nutzung von Drittplattformen, die nicht den datenschutzrechtlichen Standards der Rundfunkanstalten entsprechen

Sofern es nicht möglich ist, die datenschutzrechtlichen Standards für die Präsenz von Angeboten der Rundfunkanstalten auf Drittplattformen und deren Besuch durch Dritte - mit den jeweiligen Plattformbetreibern zu vereinbaren, gilt Folgendes:

Es ist *vor* Nutzung der Drittplattform *ausdrücklich* und in jedem Einzelfall zu prüfen, ob der redaktionelle Mehrwert oder Marketing-Mehrwert gegenüber bekannten

Datenschutz-mängeln, die insbesondere die Nutzer dieser Angebote treffen können, tatsächlich überwiegt.

Die meisten der größeren Anbieter von Social Media genügen leider momentan weder dem deutschen und dem europäischen Datenschutzrecht noch den Standards der ARD-Datenschutzbestimmungen. Einzelne Datenschutzbeauftragte vertreten die Auffassung, dass Unternehmen, die diese Plattformen zum Beispiel für Fanpages nutzen, auch für Datenschutzverstöße der Betreiber der Plattformen verantwortlich sind und gegebenenfalls auf Unterlassung der Nutzung in Anspruch genommen werden könnten. Dieser Position folgt der AK DSB in dieser Allgemeinheit nicht. Nicht genutzt werden sollten aber solche Dienste der Plattformbetreiber, bei denen Nutzerdaten ohne ausdrückliche Zustimmung ins außereuropäische Ausland übertragen werden. Dies trifft insbesondere auf Dienste zur Reichweitenmessung, wie beispielsweise „Insight“ von Facebook, zu.

Wegen der bekannten Einschränkungen bei der Einhaltung der deutschen Datenschutzgesetze und der ARD/ZDF/DLR-Standards sollte bei einem Link zu Facebook, Twitter, Google o.ä. immer ein deutlicher Hinweis zum Datenschutz platziert werden. Mit diesen Hinweisen ist der Nutzer dann ausreichend informiert und kann selbst entscheiden, ob er den Link auf die Drittplattform betätigt, sich dort erstmals registriert oder einloggt, um das Social-media-Angebot der Rundfunkanstalt auf dieser Drittplattform zu nutzen.

Hier sind verschiedene Varianten denkbar: Bei allen Varianten sollte jedoch darauf hingewiesen werden, dass die Nutzungsbedingungen des Anbieters nicht den Datenschutzstandards der Rundfunkanstalt entsprechen. Zudem sollten dem Nutzer Hinweise gegeben werden, wie er seine Privatsphäre und seine persönlichen Daten auch bei Facebook, Twitter, Google u.a. schützen kann.

Variante 1: Verlinkung auf Zwischenseite:

Bei Anklicken des Facebook-Links kommt man zunächst auf eine Zwischenseite, die den Datenschutzhinweis enthält:

► BR-online ► Das Erste ► report MÜNCHEN ► Jetzt neu

Jetzt neu
report MÜNCHEN ist bei Facebook!

Hinweis: Facebook ([Was ist das?](#)) hält die Datenschutz-Standards von BR-online leider nicht ein. Wie Sie Ihre Privatsphäre bei Facebook und anderen Sozialen Netzwerken bestmöglich schützen können, erfahren Sie [hier](#).

■ [Zu report MÜNCHEN auf Facebook: Diskutieren Sie mit!](#)
[\[www.facebook.com/reportMuenchen\]](http://www.facebook.com/reportMuenchen)

Variante 2: Hinweis zu Datenschutz/Datensicherheit unmittelbar neben dem „Facebook“-Kasten

BR-Sport bei Facebook

Stichwort Sicherheit

Was Sie in Sachen Datenschutz und Persönlichkeitsrechte rund um Facebook & Co. wissen sollten

► **Safer Internet:** Web 2.0 auf Nummer sicher [Ratgeber]

Jedes Facebook-Mitglied hat eine eigene Seite - ein Profil - auf der es sich vorstellen sowie Fotos und Videos hochladen kann. Auf der Pinnwand kann man persönliche Nachrichten hinterlassen und den Freunden mitteilen. Außerdem bekommt man selbst Neuigkeiten von seinen Freunden ebenso auf seine Startseite geliefert wie von abonnierten Fanseiten.

BR-Sport bei Facebook

Facebook

"Blickpunkt Sport" und "Heute im Stadion"



"BR-Sport" ist die gemeinsame Fanseite von "Blickpunkt Sport" und "Heute im Stadion" im Freundschafts-Netzwerk Facebook. Hier geht's direkt zu unserer Facebook-Seite!

[► www.facebook.com/BRsport]

Variante 3: Popup mit Hinweise zum Datenschutz bei Anklicken des Facebook-Links

Facebook - wer wie was?

Stichwort Sicherheit



► **Safer Internet:** Web 2.0 auf Nummer sicher [Ratgeber]

Jedes Facebook-Mitglied hat eine eigene Seite - ein Profil - auf der es sich vorstellen sowie Fotos und Videos hochladen kann. Auf der Pinnwand kann man persönliche Nachrichten hinterlassen oder im Freundeskreis Einladungen verschicken. Außerdem bekommt man Neuigkeiten von seinen Freunden ebenso auf seine Startseite geliefert wie von abonnierten Fanseiten.

Der BR bei Facebook

Auf Fanseiten der BR-Sendungen posten die Macher Sendungsinfos - und laden Sie ein, Kommentare und Ideen beizusteuern:

- [BAYERN 3-Frühaufrichter](#)
- [quer](#)
- [on3](#)
- [Zündfunk](#)
- [Abendschau](#)
- [ARD mittagsmagazin](#)
- [report MÜNCHEN](#)
- [Blickpunkt Sport / Heute im Stadion](#)
- [filmtonart](#)
- [ARD-Musikwettbewerb](#)
- [Bayern 1-Sommerreise](#)
- [Alttinger mittendrin](#)

Stichwort Sicherheit
Jedes Facebook-Mitglied...

E. Maßnahmen zur Daten-/Informationssicherheit

Damit der Datenschutz als rechtliches Ziel erreicht werden kann, sind technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten insbesondere vor Missbrauch, aber auch vor Verlust und Verfälschung erforderlich. Diese Maßnahmen müssen unter Berücksichtigung der gesetzlichen Regelungen, des Standes der Technik und der Kosten ein Schutzniveau gewährleisten, das mit Blick auf die von der Verarbeitung ausgehenden Risiken und die Art der zu schützenden Daten angemessen ist.

In der Regel unterscheiden sich die Maßnahmen je nach Ausgestaltung des Angebots und nach den Besonderheiten in der Rundfunkanstalt.

I. Angebote auf „eigenen“ Webservern

- Regelungen zu Datenschutz und IT-Sicherheit in der eigenen Rundfunkanstalt
- Umsetzung technisch und organisatorischer Maßnahmen

II. Angebote auf Webservern federführender Landesrundfunkanstalt

- In der ARD abgestimmte Regelungen in Form von Vereinbarungen z.B. Anforderungen an Web-Anwendungen und Web-Server im ARD CN

III. Angebote auf Webservern von Dritten, mit denen Verträge abgeschlossen werden

- Regelungen Vertragsbestandteil
- Einholung einer Bestätigung der Umsetzung von Sicherheitsmaßnahmen durch Abforderung Ausfüllung von Checklisten

IV. Angebote auf Webservern von Dritten ohne Einfluss auf die Sicherheit der Daten

- Erstellung und Abstimmung von Entscheidungskriterien für die Nutzung von Social Media ohne vertraglichen Einfluss in den einzelnen Häusern
- Risiken müssen bewertet und Verfahren zur Behandlung von Sicherheitsvorfällen wie z. B. Datenschutzverletzungen und Verfälschung von Informationen etabliert werden.

Regelmäßig sind die Maßnahmen zur Informationssicherheit gemeinsam mit den für IT-Sicherheit Verantwortlichen zu erarbeiten.

Ausführliche Hinweise sind beispielsweise in den folgenden Dokumenten enthalten.

- Sicheres Bereitstellen von Webangeboten (vgl. https://www.bsi.bund.de/ContentBSI/Themen/Internet_Sicherheit/WWW/Webserver/isi-web-server.html)
- Baustein B 5.4 „Webserver“ BSI-IT-Grundschutz-Katalog (vgl. <https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b05/b05004.html>)
- Anforderungen an Web-Anwendungen und Web-Server im ARD CN

Beispielhaft sei insbesondere auf folgende Datensicherheitsaspekte hingewiesen:

- **Sicherheit von Datenübertragung und Authentifizierungsmechanismen**

Generell wird ein Webserver von außen über die HTTP-Schnittstelle angesprochen. Es ist auf eine ausreichende Sicherheit bei der Übertragung von personenbezogenen Daten und bei der Authentifizierung zu achten. So sollte beispielsweise beim Übertragungsvorgang sichergestellt sein, dass die übermittelten Daten im Kommunikationskanal zwischen dem Webbrowser des Nutzers und der Web-Anwendung des Dienstbetreibers verschlüsselt werden. Die Verschlüsselung HTTPS muss sich auf alle Daten incl. der Login-Daten beziehen.

- **Sicherheit der Inhalte und Anwendungen auf dem Webserver**

Um die Inhalte und Anwendungen auf dem Server vor unbefugtem Zugriff oder Veränderung zu schützen, ist es wichtig, die Rechte der verschiedenen beteiligten Benutzer klar festzulegen. Die organisatorische und technische Realisierung der Trennung zwischen verschiedenen Benutzern, die eventuell Inhalte auf dem Server einstellen bzw. pflegen dürfen, oder gar zwischen verschiedenen Webangeboten, die gemeinsam auf einem Server beheimatet sind, ist ein wichtiger Aspekt der Sicherheit eines Webangebots.

- **Technische Sicherheit des Webserver und der Webanwendung**

Die Kompromittierung (= Angriff oder Schädigung) eines Webserver oder einer Webanwendung kann erhebliche finanzielle Verluste oder Imageschäden nach sich ziehen. Daher sind Webserver und Webanwendungen vor Angriffen aus dem Netz (also z. B. über das Internet, aber auch aus dem Intranet heraus) zu schützen. Dabei müssen auch Schwachstellen des verwendeten Betriebssystems oder anderer verwendeter Software-Produkte berücksichtigt werden.

- **Berücksichtigung von Datenschutz und IT-Sicherheitsaspekten bei Verträgen mit externen Dienstleistern, die auch mit personenbezogenen Daten der Nutzer arbeiten**

Sind externe Dienstleister mit Leistungen für das Onlineangebot der Rundfunkanstalt beauftragt, bei denen sie personenbezogenen Daten der Nutzer verarbeiten, handelt es sich nach Datenschutzrecht regelmäßig um eine sog. Auftragsdatenverarbeitung, bei der einige formale und inhaltliche Anforderungen nach dem geltenden Datenschutzgesetz einzuhalten sind. Die Rundfunkanstalt bleibt trotz Einschaltung eines Dienstleisters für die persönlichen Daten ihrer Nutzer datenschutzrechtlich verantwortlich. Die Vergabe des Auftrags hat daher unter besonderer Berücksichtigung der technischen und organisatorischen Eignung des Auftragnehmers zu erfolgen. Der Auftrag hat schriftlich zu erfolgen, wobei die Datenverarbeitung selber sowie die zugehörigen technischen und organisatorischen Maßnahmen zu beschreiben und die Anforderungen genau festzulegen sind. Zu diesen Maßnahmen gehört insbesondere auch die Gewährleistung der Auftragskontrolle. Die Auftragnehmer müssen den datenschutzrechtlich zuständigen Stellen ein entsprechendes Kontrollrecht

einräumen. Der Auftragnehmer bleibt bezogen auf die Datenverarbeitung weisungsgebunden.

Ausführliche Hinweise hierzu sind beispielsweise in folgenden Dokumenten enthalten:

- *ISO 27001 Punkt 10.2 Management der Dienstleistungserbringung von Dritten*
- ISO 27002 Punkt 10.2.1 Erbringung von Dienstleistungen*
- 10.2.2 Überwachung und Überprüfung der Dienstleistungen von Dritten*
- 10.2.3 Management von Änderungen an Dienstleistungen von Dritten*

F. Nutzung sogenannter Apps

Die Rundfunkanstalten veröffentlichen in Ergänzung zu bestimmten Sendungen bestimmte Teile ihres Angebots auch über sog. Apps (z. B. Tagesschau, Sportschau, SWR3 Elchradio, MDR Sputnik2 und BR Rundschau), die auf mobilen wie stationären Endgeräten wie Smartphones, Tablets und Fernsehern und deren Betriebssystemen aufgerufen werden können.

Hauptnutzer von Apps sind die Besitzer eines Apple iPhone. Dafür werden die Apps vom iTunes App-Store heruntergeladen. Voraussetzung zur Nutzung des App-Stores ist ein Apple-Endgerät und eine Apple ID mit folgenden Daten:

Name, Adresse, Telefonnummer, Emailadresse sowie Zahlungsdaten (Prepaid / Kreditkarte).

Apple nutzt die Daten der Apple ID laut seiner Datenschutzrichtlinie über die Vertragsabwicklung hinaus für zahlreiche weitere Zwecke wie Produktentwicklung Analyse und Forschung.

Sofern ein User die Genius-Funktion nutzt, gewährt er dem Anbieter anonymisiert Einblicke in die Nutzungsgewohnheiten, wie z.B. Anzahl der Starts der Produkte und Verwendungsdauer. Der mögliche Nutzen für Apple liegt in einem Kunden-/ Konkurrenz- und Produktvergleich.

Zudem erlaubt Apples Datenschutzrichtlinie, personenbezogene Informationen anonymisiert an fremde - auch außerhalb der EU ansässige - Dienstleister weiterzugeben, die Kundenforschung und Produktentwicklung betreiben. Nach jüngst bekannt gewordenen Datenskandalen kann nicht ausgeschlossen werden, dass die von Apples bzw. anderen Anbietern in ihren Datenschutzrichtlinien bzw. Nutzerhinweisen angekündigten Datenverwendungen nicht abschließend sind. Darauf sollten die Rundfunkanstalten in geeigneter Form hinweisen, zugleich aber darauf hinweisen, dass diese Datenverarbeitung nicht in ihrer Verantwortung liegt.

Etwas anderes gilt für die Nutzerdaten in einer App, die von dem App-Entwickler / Anbieter, also der Rundfunkanstalt, verarbeitet werden. Hier gilt Folgendes:

Es sollten ausführliche Datenschutzhinweise, die nicht versteckt sind und eine Kontaktmöglichkeit beinhalten, bereitgestellt werden.

Außer Zählpixeln und etablierter Webseitenprotokollierung sollte keine Protokollierung von Nutzerdaten stattfinden.

Die Apps sollten auch in alternativen App-Stores bereitgestellt werden.

Es sollte Möglichkeiten zum direkten Download geben.

Es sollten Web-Apps statt nativer Apps verwendet werden.

Im Hinblick auf Datensparsamkeit und Datensicherheit sollten die Protokolldaten maximal 7 Tage gespeichert werden. Anlassbezogen können die Daten mit Zustimmung der/des Datenschutzbeauftragten im Einzelfall bei Bedarf auch länger gespeichert werden.

ANHANG: Glossar

1 App

„App“ ist die Kurzform für das englische Wort „Application“ und lässt sich mit „Anwendung“ übersetzen. Eine App ist eine Software, die auf mobilen wie stationären Endgeräten wie Smartphones, Tablets und Fernsehern und deren Betriebssystemen läuft.

Web App

Eine Anwendung, bei der im Zuge der Nutzung alle oder nur bestimmte Teile der Applikation aus dem Web geladen werden. Daher kann diese Anwendung in der Regel auf allen internetfähigen Endgeräten ausgeführt werden.

Natives App

Eine Anwendung, die nur auf einem bestimmten Endgeräte-Typ und dessen Betriebssystem lauffähig ist, wie z.B. auf dem iPhone.

2 Datenschutz

Der Datenschutz hat das Ziel, jeden einzelnen Menschen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 BDSG).

.Datenschutz ist die Menge aller Vorkehrungen zur Verhinderung unzulässiger Informationsverarbeitung und umfasst jede Phase vom Beschaffen der Information über die Erfassung und Zusammenstellung bis zur Weitergabe oder Nutzung sowie der Veränderung oder Löschung.

3 Datensicherung und Datensicherheit

Damit der Datenschutz als rechtliches Ziel erreicht werden kann, sind technische und organisatorische Maßnahmen erforderlich. Sie werden mit den Begriffen Datensicherung und Datensicherheit umschrieben. Während mit dem Begriff Datensicherung die Maßnahmen gemeint sind, wird die Datensicherheit als das Ziel bezeichnet, das durch Datensicherungsmaßnahmen erreicht werden soll.

4 Datenverarbeitung

Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten (§ 3 Abs. 4 Satz 1 BDSG).

5 Fanpages

Fanpages sind Facebookseiten, auf denen sich bspw. Unternehmen, Künstler oder Politiker darstellen und die in ihrem Aufbau und ihrer Funktion im Wesentlichen Facebookseiten privater Nutzer gleichen.

6 Personenbezogene Daten

Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse, die sich auf eine bestimmte oder bestimmbare Person beziehen. Im zuletzt genannten Fall spricht man auch von personenbeziehbaren Daten. Nach der Rechtsprechung des Europäischen Gerichtshofes und zahlreicher deutscher Gerichte ist die IP-Adresse eines Nutzers ein personenbezogenes Datum. Dieser herrschenden Auffassung schließt sich der AK DSB an. Die sog. statische IP-Adresse ermöglicht ohnehin stets eine Bestimmung des Anschlussinhabers. Über die sog. dynamische IP-Adresse ist eine Bestimmung des Anschlussinhabers mit verhältnismäßigem Aufwand der datenverarbeitenden Stelle tatsächlich durchführbar, zumindest theoretisch stets möglich.

Sensible personenbezogene Daten

Sensible personenbezogene Daten sind z.B. Angaben über die ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben (§ 3 Abs. 9 BDSG).

7 Recht auf informationelle Selbstbestimmung

Grundsätzlich soll im Rahmen des aus Art. 2 Abs 1, 1 Abs. 1 Grundgesetz (GG) abgeleiteten Rechts auf informationelle Selbstbestimmung jeder Einzelne selbst bestimmen können, welche Daten er von sich gegenüber wem preisgibt.

8 Social Media

Social Media bzw. Soziale Medien bezeichnet eine Vielfalt digitaler Medien und Technologien (Social Software), die es den Nutzern ermöglicht, sich untereinander auszutauschen und mediale Inhalte einzeln oder in Gemeinschaft zu gestalten.

9 Soziale Netzwerke

Soziale Netzwerke sind Netzgemeinschaften, die technisch durch Web 2.0 Anwendungen oder Portale unterstützt werden.

Bestands- und Nutzungsdaten bei sozialen Netzwerken

Bestandsdaten sind Daten, die für die Begründung der Mitgliedschaft in den sozialen Netzwerken erforderlich sind (vgl. § 14 Abs. 1 TMG).

Nutzungsdaten sind Daten, die die Aktivitäten im Sozialen Netzwerk ermöglichen (Merkmale zur Identifikation der Nutzer, Angaben über Beginn und Ende sowie Umfang der jeweiligen Nutzung und Angabe über die vom Nutzer in Anspruch genommenen Angebote, § 15 Abs. 1 TMG).

Inhaltsdaten bei sozialen Netzwerken

Inhaltsdaten sind alle personenbezogenen Daten der Nutzer, die sie selbst auf der Plattform des sozialen Netzwerks veröffentlichen und die nicht Bestands- oder Nutzungsdaten sind.

10 User generated content

Inhalte, die nicht vom Anbieter eines Webangebots, sondern von dessen Nutzern erstellt werden.

11 Widget

Unter Widgets werden Komponenten eines Fenstersystems verstanden. Es handelt sich um kleine Elemente auf dem Desktop. Sie können z.B. den Posteingang von E-Mail-Konten, die Uhrzeit, aktuelle Verkehrs- und Wettermeldungen anzeigen oder aktualisierbare Nachrichtenschlagzeilen. Grundlage eines Widgets ist eine sog. Widget-Engine, eine Software, die die Voraussetzung für die Nutzung von Widgets bildet. Widget-Engines werden z.B. von Apple, Google, Microsoft angeboten.

12 Zweckbindung

Grundsätzlich dürfen personenbezogene Daten nur für die Zwecke verarbeitet werden, für die sie erhoben wurden.