DÜSSELDORFER KREIS
Aufsichtsbehörden für
den Datenschutz im
nicht-öffentlichen Bereich

Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste

Die Orientierungshilfe richtet sich an die Anbieter von Smart-TV-Diensten und -Produkten. Hierzu zählen insbesondere Gerätehersteller, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und Anbieter von HbbTV-Angeboten. Die Orientierungshilfe gibt einen Überblick über die datenschutzrechtliche Bewertung durch die Aufsichtsbehörden.

Redaktionelle Bearbeitung:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de
Tel.: 0981/53-1300
Fax: 0981/53-5300

Hinweis:
Dieser Orientierungshilfe wurde in der Sitzung des Düsseldorfer Kreises vom 15./16. September 2015 zugestimmt.

Stand:
September 2015, Version 1.0

Inhaltsverzeichnis

1. Einleitung

Fernsehgeräte der ersten Generation waren reine Empfangsgeräte. Programme wurden zunächst terrestrisch, später über Kabel und Satellit ausgestrahlt. Sendeschemata, Zusatz- oder Hintergrundinformationen zu dem Programm konnte das Fernsehpublikum durch Zeitungen oder Zeitschriften zur Kenntnis nehmen. Reaktionen zum Programm erfolgten auf getrennten Kommunikationswegen wie Brief, Telefon oder E-Mail. Parallel dazu entwickelte sich das Internet mit der Möglichkeit der unmittelbaren Kommunikation in alle Richtungen. Die rasant fortschreitende Konvergenz der Medien führt dazu, dass das Fernsehen, der Hörfunk und die Kommunikation über das Internet zusammenwachsen und der Markt insofern darauf reagiert, als - von der Fernsehseite aus betrachtet - mittlerweile fast ausschließlich Geräte angeboten werden, die diese Funktionalitäten zusammenführen.

Da nach der Verbindung eines „smarten“ Fernsehgerätes mit dem Internet nicht mehr nur (Rundfunk-) Signale empfangen werden, sondern vielmehr ein Rückkanal zu den jeweiligen Diensteanbietern existiert, stellen sich aus datenschutzrechtlicher Sicht zahlreiche Fragen, insbesondere, wann und welche personenbezogenen Daten bei Nutzung der unterschiedlichen Angebote fließen, wer diese Daten zu welchen Zwecken erhält, ob eine Erlaubnis für das Erheben und die weitere Verwendung der Daten existiert, ob die Datenschutzgrundsätze eingehalten werden und inwieweit technisch-organisatorische Maßnahmen dem jeweiligen Schutzbedarf entsprechen.

Diese Orientierungshilfe richtet sich an die Anbieter von Smart-TV-Diensten, insbesondere Geräteherstellern, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und von HbbTV-Angeboten. Sie enthält nach Beschreibung der relevanten Begriffe (Kapitel 2) einen kurzen Überblick über die Struktur der Smart-TV-Nutzung einschließlich der beteiligten Anbieter (Kapitel 3), der gesetzlichen Grundlagen für die jeweilige Kommunikation (Kapitel 4 bis 6) und daraus folgend eine Darstellung der konkreten datenschutzrechtlichen und technisch-organisatorischen Anforderungen an Smart-TV-Dienste (Kapitel 7).

2. Begriffsbestimmungen

2.1 Auftragsdatenverarbeiter

Nimmt eine andere Stelle Datenverarbeitungen im Auftrag des eigentlichen Diensteanbieters bzw. der eigentlichen verantwortlichen Stelle und somit streng weisungsgebunden vor, so werden diese Datenverarbeitungen dem Auftraggeber zugerechnet. Den Auftraggeber treffen vielfältige Sorgfalts- und Kontrollverpflichtungen, die in § 11 Bundesdatenschutzgesetz (BDSG) dargestellt und geregelt sind. Dem Auftragnehmer ist es untersagt, personenbezogene Daten für andere Zwecke als diejenigen der verantwortlichen Stelle zu erheben und zu verwenden. Obwohl er verpflichtet ist, die Weisungen des Auftraggebers zu befolgen, obliegt es ihm, den Auftraggeber unverzüglich darauf hinzuweisen, wenn und soweit eine Weisung gegen Datenschutzbestimmungen verstößt.

Kein Auftragsdatenverarbeitungsverhältnis i.S.d. § 11 BDSG liegt jedoch vor, wenn ganze Funktionalitäten ausgelagert werden und eine andere Stelle personenbezogene Daten in eigener Verant-

wortung erhebt und verwendet. Dann ist die andere Stelle als Dritter tätig und unterliegt deshalb den datenschutzrechtlichen Anforderungen in eigener Verantwortung.

2.2 HbbTV

Die Abkürzung HbbTV steht für Hybrid Broadcasting Broadband TV und bedeutet, dass sowohl das Rundfunksignal (Broadcasting) als auch das Breitbandinternet (Broadband) genutzt werden, um dem Fernsehzuschauer neben der Rundfunksendung auch zahlreiche weitere Zusatzinformationen anzubieten. Dabei wird mittels des Rundfunksignals entweder der (erste) Inhalt einer HbbTV-HTML-Seite oder eine HTTP-URL mitgeliefert, anhand derer ein Smart-TV eine spezielle HbbTV-HTML-Seite über das Internet von einem Server des Fernsehsenders laden kann.

Derzeit werden über HbbTV z.B. Zusatzinformationen zum TV-Programm durch die Sender zur Verfügung gestellt, ein Zugriff auf Mediatheken und soziale Netzwerke ermöglicht und elektronische Programmzeitschriften sowie sonstige Seiten zum Aufruf angeboten. Ferner ist denkbar, z.B. Merchandising-Artikel zu einem Spielfilm parallel über HbbTV anzubieten oder Zuschauerumfragen in Echtzeit zu schalten. Darüber hinaus könnte über HbbTV die Schaltung von interessenbezogener Werbung (nicht nur durch die Sender, sondern auch durch Dritte) bei direkter Möglichkeit zur Reichweitenmessung und Nutzungsanalyse erfolgen.

2.3 Lineares Verfahren/Karussellverfahren

Das Rundfunksignal enthält für die Bereitstellung von HbbTV-Inhalten eine Datentabelle (Application Information Table – AIT), anhand deren Einträge der Transportweg des HbbTV-Contents (z.B. der Startseite) definiert wird. Ist hierfür das „DSMCC Object Carousel“ eingetragen, werden darstellbare Inhalte über das lineare Rundfunksignal ausgeliefert. In diesem Fall ist es im Vergleich zu dem Broadband-Verfahren, das Inhalte der Startseite über den Internet-Rückkanal lädt, nicht notwendig, dass Nutzungsdaten vor dem Drücken des Red Buttons (siehe 2.5) übertragen werden. Sollen dynamische oder personalisierte Inhalte nach Drücken des Red Buttons angeboten werden, könnte über das lineare Verfahren der Inhalt der verkleinerten Darstellung der HbbTV-Startseite (bestehend z.B. aus HTML, CSS und Grafikdateien) ausgeliefert werden; die anderen (dynamischen) Inhalte könnten dann in der HbbTV-Anwendung gekapselt und damit erst bei Erkennen des Events, das mit dem Drücken des Red Buttons zusammenhängt, aktiviert werden und über den Internet-Rückkanal könnten sodann weitere Inhalte geladen werden.

2.4 Personenbezogene Daten

Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Hiernach gelten alle Informationen, die einen Rückschluss auf eine Person erlauben, mindestens als bestimmbar, damit aber auch als personenbezogen und datenschutzrelevant. Bei der Frage, ob eine Bestimmtheit oder Bestimmbarkeit einer natürlichen Person gegeben ist, sind alle Mittel zu be-

rücksichtigen, die vernünftigerweise entweder von der datenverarbeitenden Stelle oder einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen[1]. Gerade im Online-Umfeld bedarf es hierbei nicht zwingend einer Individualisierung mittels des bürgerlichen Namens, vielmehr genügt es, wenn eine Person „singularisiert", d.h. als Individuum herausgehoben wird[2].

Speziell im Zusammenhang mit Smart-TV-Diensten stehende personenbezogene Daten sind u.a.

- **die IP-Adresse** des Nutzers, die - bei dynamischen IP-Adressen in Verbindung mit der Zeitangabe - nach Ansicht der Datenschutzaufsichtsbehörden ein personenbezogenes Datum und auch bei Smart-TV-Diensten für die Internetkommunikation notwendig ist und
- **Geräte-IDs**[3], die dauerhaft mit dem Gerät verbunden sind und regelmäßig einer Person zugeordnet werden können (z.B. bei Registrierung).

Dass unter Umständen mehrere Personen ein Fernsehgerät nutzen, führt nicht dazu, dass bei den genannten Informationen nicht mehr von einem Personenbezug auszugehen ist. Dem Dienstanbieter ist (zunächst) nicht bekannt, ob sich hinter einer IP-Adresse oder Geräte-ID wie der MAC-Adresse oder der Seriennummer nur ein Nutzer der Smart-TV-Dienste oder mehrere Personen verbergen, welche die Dienste über die gleiche Kennung in Anspruch nehmen. Da dies nicht erkennbar ist und auch nicht ausgeschlossen werden kann, gehen die Datenschutzbehörden in Europa davon aus, dass ein einzelner Nutzer jedenfalls hinter einem relevanten, hohen Prozentsatz der Kennungen steckt.[4] Daher ist der Gesamtbestand der Daten als personenbezogen zu behandeln. Darüber hinaus ist es auch möglich, bei Heranziehung des Nutzungsverhaltens Unterscheidungen zu tätigen (z.B. kann anhand der gesehenen Sendungen das Geschlecht und ggf. das Alter eingeschätzt werden) und so die jeweils konkrete Person zu individualisieren. Bei einigen Geräten lassen sich außerdem Profile für die einzelnen Nutzer einrichten, wobei dann in der Regel **personalisierte IDs** verwendet werden, die zweifellos als personenbezogene Daten einzustufen sind.

Neben den dargestellten „speziellen" Daten können mittels der Smart-TV-Dienste zahlreiche weitere Arten personenbezogener Daten erhoben und verwendet werden, wie z.B.:

- **Audiodaten** mit Stimmaufnahmen
- **Foto- und Filmaufnahmen** einer Person
- **Informationen über die Smart-TV-Dienste-Nutzung**, d.h. Auskunft darüber, welche Funktionalität und welches Angebot vom Nutzer in Anspruch genommen wurden
- **Fernsehverhalten,** d.h. Informationen zu den angesehenen Fernsehinhalten (Fernsehprogramm, Zeitpunkt und Dauer)

[1] Vgl. Art. 2 a) Richtlinie 95/46/EG und Erwägungsgrund 26; Stellungnahme 4/2007 zum Begriff „personenbezogener Daten" der Artikel 29-Gruppe (WP 136, S.17).
[2] WP 136, S. 16
[3] Vgl. WP 136, S.16, WP 202, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, S.10; „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter" des Düsseldorfer Kreises vom Juni 2014, S.5
[4] vgl. WP 136, S. 20

- **Registrierungsdaten**, z.B. Name, E-Mail-Adresse, Heimatregion
- **Zahlungsdaten,** z.B. Bankverbindungen, Kreditkartendaten

2.5 Red-Button

Ist ein HbbTV-Angebot verfügbar, wird dies dem Nutzer derzeit anhand eines kleinen Ausschnittes der HbbTV-Startseite am (unteren) Bildschirmrand angezeigt. Zugleich wird er aufgefordert, für die Inanspruchnahme des HbbTV-Angebots die rote Taste, den sog. Red Button, auf der Fernbedienung zu drücken, um die Startseite im Vollbildmodus aufrufen zu können.

2.6 Smart-TV

Smart-TV (= intelligenter Fernseher), auch Hybrid-TV genannt, ist die Bezeichnung für Fernsehgeräte mit Computer-Zusatzfunktionen und insbesondere Internet-Fähigkeit. Sogenannte smarte Fernsehgeräte verfügen neben der TV-Funktion u.a. über Zusatzschnittstellen wie z.B. USB und WLAN und meist über die HbbTV-Funktionalität (vgl. Definition HbbTV). Dadurch ist es mit diesen Geräten möglich, nicht nur Fernsehprogramme zu empfangen, sondern auch im Internet zu surfen, Filme in Echtzeit oder aus Online-Videotheken abzurufen und über manche Geräte Videotelefonate zu führen. Darüber hinaus können diese Geräte, wie manche „normale“ Geräte bisher auch schon, auf Video-, Musik- und Bilddateien zugreifen, die auf einem PC oder USB-Stick gespeichert sind.

2.7 Telemedien

Telemedien sind nach § 1 Abs. 1 Telemediengesetz (TMG) alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages (RStV) sind.

Bei einer elektronisch im Wege der Telekommunikation erbrachten Dienstleistung, bei der Inhalte bereitgestellt werden, handelt es sich um einen elektronischen Informations- und Telekommunikationsdienst im o.g. Sinne.[5] Keine direkte Anwendung findet das TMG allerdings, wenn es sich dabei um Dienste handelt, die ganz in der Übertragung von Signalen (ohne Inhaltsangebot) liegen, wenn eine Individualkommunikation zwischen dem TK-Diensteanbieter (oder Dritten) und TK-Kunden, in deren Rahmen der TK-Diensteanbieter (oder Dritte) gegenüber TK-Kunden eine Inhaltsleistung erbringen[6] im Raum steht oder wenn ein linearer Informations- und Kommunikationsdienst angeboten wird, der eine für die Allgemeinheit und zum zeitgleichen Empfang bestimmte

[5] Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 1 TMG Rn.4
[6] Vgl. BT-Drs. 16/3078, 13

Veranstaltung und Verbreitung von Angeboten in Bewegtbild oder Ton entlang eines Sendeplans unter Benutzung elektromagnetischer Schwingungen (Rundfunk)[7] darstellt.

In der Regel ist somit dann von einem Telemediendienst auszugehen, wenn

- Inhalte (wie Bilder, Töne, Zeichen) online übertragen werden,
- die übertragende Stelle selbst nicht nur als neutraler Übermittler, sondern (auch) als Inhaltsanbieter tätig ist,
- die Inhaltsleistung zeitlich von der Übertragung trennbar ist und
- es sich nicht um einen linearen Dienst handelt, der nur anhand eines bestimmten Sendeplans zeitgleich von der Allgemeinheit empfangen werden kann.

2.8 Verantwortliche Stelle und Betroffene, Diensteanbieter und Nutzer

Verantwortliche Stelle ist nach der Definition in § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Als **Betroffenen** definiert das BDSG jede natürliche Person, die durch personenbezogene Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse bestimmt oder bestimmbar gemacht werden kann (§ 3 Abs. 1 BDSG).

Diensteanbieter ist gemäß § 2 Nr. 1 TMG jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert. Im Bereich der Smart-TV-Nutzung ist hier vor allem zu denken an Anbieter von HbbTV-Angeboten, Anbieter von Web-Diensten, die über das Smart-TV-Gerät abrufbar sind, sowie Betreiber von Smart-TV-Plattformen, die den Zugang zu Web-Diensten ermöglichen.

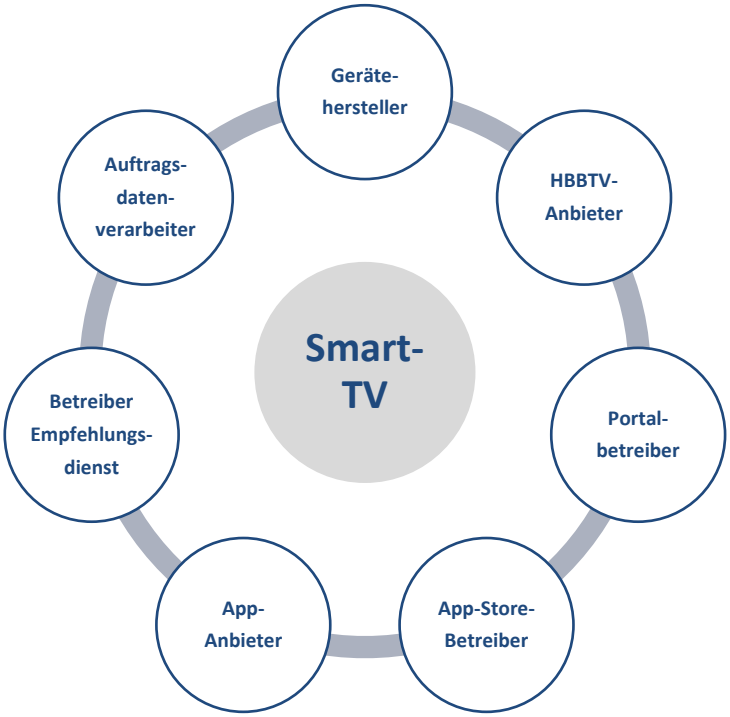
Nutzer ist jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen (§ 2 Nr. 3 TMG).

Diese unterschiedlichen Begrifflichkeiten leiten sich aus den unterschiedlichen Rechtsgrundlagen, dem BDSG und dem TMG her. Im Folgenden werden die Stellen, die mit personenbezogenen Daten umgehen (verantwortliche Stellen und Diensteanbieter) als Anbieter und die natürlichen Personen, mit deren personenbezogenen Daten umgegangen wird (Betroffene und Nutzer) als Nutzer bezeichnet (es sei denn, eine Differenzierung ist aus Gründen der Klarheit gefordert).

[7] Gem. § 47 RStV gelten bei Vorliegen eines Rundfunkdienstes die Vorschriften des TMG jedoch entsprechend.

3. Anbieter in Zusammenhang mit Smart-TV

Smart-TV-Nutzung setzt sich, wie in der folgenden Grafik dargestellt, aus vielen verschiedenen Diensten zusammen. Dabei ist zu berücksichtigen, dass die Entwicklung von Geschäftsmodellen im Zusammenhang mit Smart-TV ebenso wie die technische Entwicklung sehr dynamisch ist und diese Grafik deshalb nur eine Momentaufnahme darstellt, die sich aus den Erkenntnissen der technischen Überprüfung durch das Bayerische Landesamt für Datenschutzaufsicht in eigener örtlicher Zuständigkeit und unter Mitwirkung der für die verschiedenen Hersteller von Smart-TV örtlich zuständigen Aufsichtsbehörden in den Monaten Dezember 2014 und Januar 2015 ergeben haben.



Da die datenschutzrechtlichen Grundlagen für die Beziehung zwischen dem Nutzer und den jeweiligen Anbietern von Smart-TV-Diensten unterschiedlich sind, ist es erforderlich, zunächst konkret festzustellen, wer welche Dienste in welcher Verantwortlichkeit anbietet, um dann prüfen zu können, welche gesetzlichen Grundlagen für den jeweiligen Dienst und den damit zusammenhängenden Datenumgang bestehen. Im Folgenden werden deshalb zunächst die in der obigen Grafik benannten Akteure näher dargestellt und bereits nach ihrer jeweiligen Verantwortlichkeit eingestuft. Welche Anforderungen einen Akteur in der Regel treffen und welche Empfehlungen die Aufsichtsbehörden für den konkreten Akteur aussprechen, wird nach einem allgemeinen datenschutzrechtlichen Überblick in Kapitel 7 näher erläutert.

Die folgende Aufzählung benennt die Akteure nach Funktionen getrennt; jedoch ist es nicht unüblich, dass eine Stelle auch mehrere Funktionen wahrnimmt (z.B. Gerätehersteller ist auch Portalbetreiber).

3.1 Gerätehersteller

Gerätehersteller produzieren nicht nur das Gerät, sondern führen bei der Nutzung des Gerätes als Smart-TV, d.h. nachdem das Gerät mit dem Internet verbunden wurde, häufig zumindest Update-Checks durch und spielen bei Bedarf neue Updates ein. Zudem erstellen sie oftmals Statistiken über die Bedienung des Gerätes, um z.B. die Benutzerfreundlichkeit verbessern zu können. Gerätehersteller sind für eine damit verbundene Erhebung und Verwendung personenbezogener Daten (z.B. Geräte-ID, IP-Adresse) verantwortliche Stelle. Gerätehersteller, die Telemedien anbieten, agieren zugleich als Telemedien-Diensteanbieter.

3.2 HbbTV-Anbieter

Soweit (Programm-)Anbieter Fernseh- und Hörfunkprogramme anbieten, ist dieser Vorgang nicht Gegenstand dieser Orientierungshilfe. Bietet der Sender selbst oder ein von ihm beauftragtes Unternehmen (vgl. Kapitel 2.1) daneben HbbTV-Zusatzangebote an, ist der Sender jedoch (auch) Telemedienanbieter und verantwortliche Stelle für den mit dem Zusatzangebot verbundenen Datenumgang. Mögliche weitere Konstellation ist, dass eine Gesellschaft, z.B. die für Multimedia-Inhalte zuständige Gesellschaft, die zu der gleichen Unternehmensgruppe wie die Sendergesellschaft gehört, das HbbTV-Angebot in eigener datenschutzrechtlicher Verantwortlichkeit bereitstellt. In diesem Fall ist die (Multimedia-)Gesellschaft selbst Diensteanbieter und verantwortliche Stelle für den Datenumgang im Zusammenhang mit dem HbbTV-Angebot.

3.3 Portalbetreiber

Einige Smart-TVs bieten einen Zugang zu einem eigenen oder einem von dritter Stelle betriebenen Smart-TV-Portal an, über das z.B. vorinstallierte Apps (auch in Form von Verlinkungen) genutzt werden können oder auf App-Stores zugegriffen werden kann. In einigen Fällen ist eine Registrierung des Nutzers erforderlich, um das Portal nutzen zu können. Zudem werden zum Teil Nutzungsanalysen durchgeführt. Über die TV-Plattformen können u.U. zusätzlich weitere Akteure, wie z.B. ein App-Store-Betreiber oder App-Anbieter angesprochen werden. Die Betreiber des Portals agieren als verantwortliche Stelle und Diensteanbieter, soweit sie selbst in eigener Verantwortung personenbezogene Daten erheben und verwenden.

3.4 App-Store-Betreiber

Neben den vorinstallierten Apps wird dem Nutzer bei vielen Plattformen die Möglichkeit gegeben, selbst Apps über einen App-Store zu installieren. Wird der App-Store nicht von dem Portalbetreiber selbst betrieben, handelt es sich bei dem App-Store-Betreiber um einen weiteren Akteur, der jedenfalls im Falle einer Registrierung und Nutzung des App-Stores personenbezogene Daten zu eigenen Zwecken erhebt und verwendet. In diesem Fall ist der App-Store-Betreiber verantwortliche Stelle und Diensteanbieter.

3.5 App-Anbieter

Handelt es sich bei den (vorinstallierten oder im Nachhinein heruntergeladenen) Apps um „Fremd-Anwendungen“, also nicht solche des Portalbetreibers, ist der jeweilige App-Anbieter als eigenständiger Diensteanbieter und verantwortliche Stelle einzustufen.

Ebenfalls sind App-Anbieter auch diejenigen Stellen, die Smartphone- oder Tablet-Apps für eine Kommunikation mit dem Smart-TV anbieten (z.B. Fernaufnahmefunktion, Second Screen). Oft werden diese Apps von den Geräteherstellern selbst entwickelt und angeboten.

3.6 Betreiber von Personalisierungsdiensten (Empfehlungsdienste)

Häufig werden dem Nutzer Empfehlungsdienste angeboten, die auf Basis des jeweiligen Nutzerverhaltens Vorschläge für weitere Angebote oder Fernsehsendungen machen, die den Vorlieben des Nutzers entsprechen. Die Vorlieben des Nutzers werden dabei ermittelt, indem z.B. bei der Bedienung des -online betriebenen - elektronischen Programmführers (EPG) erfasst wird, welche Sendungen ein Nutzer aus diesem heraus anklickt, aufnimmt, vormerkt etc. oder aber indem analysiert wird, welche Inhalte von einem externen Speichermedium aus auf das Gerät eingespielt oder wie welche Smart-TV-Dienste genutzt werden. Der Betreiber eines Empfehlungsdienstes ist als verantwortliche Stelle und Diensteanbieter einzustufen.

3.7 Auftragsdatenverarbeiter

In vielen Fällen werden Dienstleister eingeschaltet, um bestimmte Datenverarbeitungen im Auftrag durchzuführen (= Auftragsdatenverarbeitung, vgl. Definition in Kapitel 2.1). Neben der Wartung und Pflege von Software kommen z.B. Dienstleister, die Nutzungsanalysen durchführen, in Betracht. Das weisungsgebundene Handeln wird dem Auftraggeber (= verantwortliche Stelle) zugerechnet.

4. Anwendbares Datenschutzrecht

4.1 Deutsches Datenschutzrecht

Das Bundesdatenschutzgesetz gilt als allgemeine Rechtsgrundlage bei Umgang mit personenbezogenen Daten durch Stellen mit Sitz in der Bundesrepublik Deutschland (BRD) oder eine Tätigkeit im Rahmen einer Niederlassung in der BRD ausgeführt wird, soweit nicht andere Vorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Im Zusammenhang mit der Smart-TV-Nutzung enthält das Telemediengesetz in den §§ 11 ff. datenschutzrechtliche Regelungen, die als bereichsspezifische Rechtsvorschriften den allgemeinen Datenschutzregelungen im BDSG vorgehen.

Gem. § 1 Abs. 1 Satz 1 TMG gilt das TMG „für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikations-

gesetzes (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien)." Welche Dienste als Telemedien eingestuft werden können, wurde bereits unter Kapitel 2.7 dargestellt.

Da im Zusammenhang mit Smart-TV-Angeboten regelmäßig Inhalte elektronisch übertragen werden (Webseiten, Apps etc.) und somit Telemediendienste vorliegen, sind vorwiegend das TMG und ergänzend das BDSG als allgemeines Gesetz zu beachten.[8]

4.2 Internationaler Datenverkehr

Soweit ein Anbieter, der nicht in einem Mitgliedstaat der Europäischen Union (EU) oder einem Vertragsstaat des Europäischen Wirtschaftsraumes (EWR) belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, findet das Bundesdatenschutzgesetz Anwendung (§ 1 Abs. 5 Satz 2 BDSG). Soweit ein in einem anderen Mitgliedstaat der EU oder im EWR-Bereich gelegener Anbieter personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt und dies nicht durch eine Niederlassung dieses Anbieters im Inland erfolgt, findet das Bundesdatenschutzgesetz keine Anwendung (§ 1 Abs. 5 Satz 1 BDSG), sondern das Recht des jeweiligen Mitgliedstaats der Europäischen Union oder des Vertragsstaats im EWR.[9]

Da das Telemediengesetz insoweit keine eigenen innergemeinschaftlichen Kollisionsvermeidungsnormen enthält, ist für die Anwendbarkeit dieser bereichsspezifischen datenschutzrechtlichen Regelungen auf die kollisionsrechtlichen Regelungen des Bundesdatenschutzgesetzes abzustellen. Soweit also grundsätzlich das BDSG zur Anwendung käme, im vorgelegten Fall aber aus Gründen der Subsidiarität nicht einschlägig ist, treten die bereichsspezifischen Regelungen des Telemediengesetzes an die Stelle der Vorschriften des Bundesdatenschutzgesetzes.

5. Datenschutzrechtliche Rahmenbedingungen für Smart-TV

Sowohl nach den Vorschriften des Bundesdatenschutzgesetzes als auch des Telemediengesetzes gilt der Grundsatz, dass personenbezogene Daten nur erhoben und verwendet[10] werden dürfen, soweit dies durch das Bundesdatenschutzgesetz, das Telemediengesetz oder eine andere einschlägige Rechtsvorschrift erlaubt ist oder der Nutzer eingewilligt hat (sog. Verbot mit Erlaubnisvorbehalt, vgl. § 4 Abs. 1 BDSG und § 12 Abs. 1 TMG). Wenn nicht eine dieser Voraussetzungen vorliegt, ist der Umgang mit per-

[8] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz" vom Mai 2014, Ziffer 2

[9] Weitere Ausführungen zum anwendbaren Recht finden sich in der Stellungnahme der Art. 29 Gruppe 8/2010 zum anwendbaren Recht, abrufbar unter ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf

[10] Der Begriff „Verwenden" personenbezogener Daten findet sich in den §§ 11 ff. TMG. Er umfasst das Verarbeiten und Nutzen personenbezogener Daten i.S.d. § 3 Abs. 4 und Abs. 5 BDSG. Entsprechend wird dieser Begriff vorliegend einheitlich (sowohl im Anwendungsbereich des BDSG als auch des TMG) verwendet.

sonenbezogenen Daten durch Anbieter von Smart-TV-Diensten datenschutzrechtlich unzulässig, kann durch die zuständige Datenschutzaufsichtsbehörde unterbunden und gegebenenfalls mit einem Bußgeld geahndet werden.

5.1 Erlaubnistatbestände

Bei der Nutzung von Smart-TV-Diensten stehen der Umgang mit Bestandsdaten (vgl. § 14 TMG) und Nutzungsdaten (vgl. § 15 TMG) im Fokus. Hiervon zu unterscheiden sind Inhaltsdaten. Für diese Daten gelten in der Regel die allgemeinen Datenschutzgesetze (im nicht-öffentlichen Bereich das BDSG).

5.1.1 Erlaubnistatbestände aus dem TMG

Die datenschutzrechtlichen Regelungen des Telemediengesetzes finden sich in den §§ 11 ff. In diesen Regelungen wird die Erhebung und Verwendung der Bestands- und Nutzungsdaten sowohl durch öffentliche als auch durch nicht-öffentliche Stellen (§ 1 Abs. 1 Satz 2 TMG) behandelt. Der Anwendungsbereich des TMG ist eröffnet, soweit es sich bei dem angebotenen Dienst um einen Telemediendienst gem. § 1 Abs. 1 TMG handelt.

5.1.1.1 Bestandsdaten

Gem. § 14 Abs. 1 TMG darf ein Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten). Welche personenbezogenen Daten konkret für diese Zwecke erforderlich sind, wird durch den jeweiligen Nutzungsvertrag bestimmt, der zwischen Anbieter und Nutzer abgeschlossen wird. Zu den Bestandsdaten können insbesondere Name, Anschrift, Rufnummer, Registrierungs- und Zahlungsdaten zählen.

Beispiel:
Kann sich ein Nutzer in einem Online-Portal registrieren, um eine Bewertung zu einer TV-Sendung o.ä. abzugeben, handelt es sich bei den Registrierungsdaten um Bestandsdaten.

5.1.1.2 Nutzungsdaten

Nutzungsdaten sind gem. § 15 Abs. 1 TMG die personenbezogenen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und mit dem Nutzer abzurechnen.

Das TMG definiert nicht abschließend folgende Daten als Nutzungsdaten:

- Merkmale zur Identifikation des Nutzers
- Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien

Zu den Nutzungsdaten zählen somit alle personenbezogenen Daten, die notwendigerweise zur Nutzung des Dienstes durch den Diensteanbieter erhoben und verwendet werden müssen, wie z.B. nach Auffassung der Datenschutzbehörden die IP-Adresse oder - soweit im Einzelfall erforderlich - eindeutige Kennnummern. Die Erforderlichkeit misst sich hierbei an Sinn und Zweck des jeweiligen Dienstes. Für die Erbringung des Dienstes ist dann die Erhebung und Verwendung dieser Nutzungsdaten zulässig.

Beispiel:
Ein Smart-TV lädt aus dem Internet über das HTTP-Protokoll Daten zur Erbringung eines Dienstes, zum Beispiel zur Erbringung des HbbTV-Angebotes oder zur Nutzung einer App. In diesem Zusammenhang werden z.B. die IP-Adresse, ein Zeitstempel und weitere Nutzungsdaten, die für die Erbringung des Dienstes technisch notwendig sind, zulässigerweise an den Anbieter übertragen.

§ 15 Abs. 3 TMG gestattet dem Diensteanbieter die Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung von Telemedien bei Verwendung von Pseudonymen, soweit der Nutzer nicht widerspricht.

Der Nutzer muss vom Diensteanbieter auf die Erstellung eines solchen Nutzungsprofils und die Möglichkeit, der Verwendung seiner Nutzungsdaten zu diesem Zweck widersprechen zu können, hingewiesen werden. Dies muss zumindest in der Datenschutzerklärung (vgl. Kapitel 5.2.1) geschehen. Die Widerspruchsmöglichkeit muss effektiv und angemessen sein. Es sollte daher eine direkte Opt-Out-Möglichkeit (Link, Möglichkeit des Auskreuzens) für den Nutzer vorgehalten werden, die mit möglichst einem Klick aktiviert werden kann und dazu führt, dass der Datenfluss unterbrochen wird. Die Möglichkeit, per E-Mail oder postalisch einer Nutzungsprofilerstellung gem. § 15 Abs. 3 TMG zu widersprechen, genügt nicht, da bei einem Widerspruch per E-Mail oder per Post eine Zuordnung aufgrund des Medienbruches im Allgemeinen nicht erfolgen kann. Der Widerspruch gegen die automatisierte Nutzungsprofilbildung unter Pseudonym kann im Regelfall auf technischer Ebene effektiv umgesetzt werden (z.B. Opt-Out-Cookie). Widerspricht der Nutzer der Profilbildung unter Pseudonym, so sind etwa vorhandene Profildaten zu löschen oder wirksam gem. § 3 Abs. 6 BDSG zu anonymisieren.

Die Regelungen des § 15 Abs. 3 TMG berechtigen nur den Diensteanbieter selbst oder seine Auftragnehmer zur Erstellung pseudonymer Nutzerprofile zu Werbezwecken. Eine Verwendung von Nutzungsdaten durch Dritte kann nicht auf diese Regelungen gestützt werden. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen jedoch anonymisierte Nutzungsdaten übermittelt werden (§ 15 Abs. 5 Satz 3 TMG).

Eindeutige Gerätekennungen oder auch die IP-Adresse stellen kein Pseudonym dar[11]. Diese Daten dürfen nicht in das Nutzungsprofil einfließen, da die Zusammenführung pseudonymer Nutzungsprofile mit Daten über den Träger des Pseudonyms unzulässig ist (Verstoß gegen § 15 Abs. 3 Satz 3 TMG, § 13 Abs. 4 Nr. 6 TMG).

Im Zusammenhang mit der Nutzung von Smart-TV-Diensten wird die soeben dargestellte Erlaubnis zur Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung von Telemedien bei Verwendung von Pseudonymen insbesondere in den folgenden Konstellationen genutzt:

- **Reichweitenmessung**

  Eine Nutzungsprofilerstellung unter Pseudonym gem. § 15 Abs. 3 TMG findet insbesondere zur Reichweitenmessung statt. Mittels einer Reichweitenmessung kann ein Diensteanbieter feststellen, in welchem Umfang und auf welche Weise sein Angebot genutzt wird. So kann er z.B. feststellen, wie viele Nutzer einen bestimmten Sender ansehen, wie viele davon den Red Button drücken und welche Angebote sie wie oft innerhalb der HbbTV-Plattform ansehen und nutzen.

  Auf die Voraussetzungen für die „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ hat der Düsseldorfer Kreis mit Beschluss vom 26./27. November 2009 hingewiesen.[12] Diese folgenden Voraussetzungen sind auch bei einem Einsatz im Zusammenhang mit der Nutzung von Smart-TV-Diensten einzuhalten:

  - Anonymisierung der IP-Adresse (z.B. durch Kürzen oder Überschreiben der IP-Adresse),
  - Vorhalten einer Widerspruchsmöglichkeit und wirksame Umsetzung von Widersprüchen,
  - keine Zusammenführung des Pseudonyms mit Daten über Träger des Pseudonyms,
  - Unterrichtung über Erstellung pseudonymer Nutzungsprofile und über die Widerspruchsmöglichkeit und
  - soweit ein Dienstleister eingesetzt wird, Abschluss eines Auftragsdatenverarbeitungsvertrages gem. § 11 BDSG.

- **Werbefinanzierte Dienste**

  Viele Dienste können „kostenfrei“ genutzt werden. In Wahrheit werden diese Angebote vielfach durch eine Verarbeitung von Nutzungsdaten zu Werbezwecken finanziert. Dazu kann beispielsweise auch ausgewertet werden, wie Nutzer ein HbbTV-Angebot bedienen, um ihnen

[11] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 2

[12] Beschluss „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten" vom 26./27. November 2009, abrufbar unter www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.html

möglichst passgenaue Werbung zu präsentieren. Datenschutzrechtlich ist das nur zulässig, wenn die oben genannten Voraussetzungen des § 15 Abs. 3 TMG eingehalten werden oder ein anderer Erlaubnistatbestand für den Umgang mit personenbezogenen Daten vorliegt.

Soweit Nutzungsdaten durch Diensteanbieter für die Abrechnung kostenpflichtiger Angebote verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung in den §§ 15 Abs. 2, 4 ff. TMG geregelt wird. Der Diensteanbieter darf diese Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, wenn sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.

5.1.2 Erlaubnistatbestände aus dem BDSG

Soweit es nicht um eine Datenerhebung und -verwendung auf der Anwendungsebene, sondern um eine Datenerhebung und -verwendung auf der Inhaltsebene geht, findet grundsätzlich das Bundesdatenschutzgesetz Anwendung. Ein Datenumgang auf der Inhaltsebene ist dann anzunehmen, wenn online Daten zwischen dem Nutzer und dem Anbieter ausgetauscht werden, um ein Vertrags- oder Leistungsverhältnis zu begründen, das selbst keinen Telemediendienst darstellt („Offline-Vertrag“)“). Zwar werden die Daten unter Anwendung des Smart-TV-Dienstes eingegeben und übermittelt, ermöglicht wird jedoch eine Verwendung außerhalb des Anwendungsbereichs des TMG. Bei der Erhebung und Verwendung personenbezogener Daten durch nichtöffentliche Stellen sind die §§ 27 ff. BDSG anzuwenden. Darüber hinaus können im konkreten Einzelfall spezielle Datenschutzregelungen vorrangig anzuwenden sein.

Beispiel: Im Rahmen eines HbbTV-Angebotes kann der zu einem Menü in einer gerade ausgestrahlten Kochsendung passende Wein bestellt werden. Die dann in das Bestellformular eingegebenen Daten sind nicht erforderlich für die Begründung, inhaltliche Ausgestaltung oder Änderung des „Telemedien-Vertragsverhältnisses“, aber für die „Offline-Erfüllung“ des dann geschlossenen Kaufvertrages.

5.1.3 Einwilligung

Existiert kein gesetzlicher Erlaubnistatbestand, sind Erhebung und Verwendung personenbezogener Daten nur mit einer wirksamen Einwilligung des Nutzers möglich.

Soweit eine Einwilligung in Betracht kommt, sind die Voraussetzungen für eine wirksame Einwilligung - je nachdem, ob das TMG Anwendung findet oder nicht - in § 4a BDSG und § 13 Abs. 2, 3 TMG geregelt.

Während § 4a BDSG neben der Freiwilligkeit und Informiertheit der Einwilligung grundsätzlich die Schriftform fordert, erlaubt und regelt das Telemediengesetz für Telemedien die Einholung einer elektronischen Einwilligung. Eine Einwilligung kann gegenüber dem Anbieter elektronisch erklärt werden, wenn die Vorgaben des § 13 Abs. 2 und Abs. 3 TMG eingehalten werden. Hiernach ist erforderlich, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat (z.B. durch Ankreuzen einer vorformulierten Einwilligung),
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Hierauf ist der Nutzer bereits vor Erteilung der Einwilligung hinzuweisen.

Die freiwillige Einwilligung muss vor der Datenverarbeitung durch den Nutzer abgegeben worden sein. In diesem Zusammenhang ist insbesondere auch zu beachten, dass gemäß § 12 Abs. 3 TMG i. V. m. § 28 Abs. 3b BDSG das Kopplungsverbot gilt, d.h. die verantwortliche Stelle darf den Abschluss eines Vertrages nicht von einer Einwilligung des Nutzers in die werbliche Nutzung seiner Daten abhängig machen, wenn dem Nutzer ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Hiervon ist auszugehen, wenn ein vergleichbarer gleichwertiger Dienst von einem anderen Anbieter nicht bezogen werden kann.[13]

Wenn ein Datenumgang in Klauseln geregelt wird, die gem. §§ 305 ff. Bürgerliches Gesetzbuch (BGB) nicht wirksam sind, fehlt die Rechtsgrundlage für den dort geregelten Datenumgang.

5.2 Informationspflichten

5.2.1 Datenschutzerklärung

Ein Telemedienanbieter hat gemäß § 13 Abs. 1 Satz 1 TMG den Nutzer „zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten [außerhalb der EU bzw. des EWR] (...) in allgemein verständlicher Form zu unterrichten". Nach Satz 3 des § 13 Abs. 1 TMG muss der Inhalt der Unterrichtung für den Nutzer auch jederzeit abrufbar sein. Zudem ist der Nutzer zu Beginn eines automatisierten Verfahrens, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, hierüber zu informieren (vgl. § 13 Abs. 1 Satz 2 TMG). Letztere Unterrichtungspflicht zielt insbesondere auf den Einsatz von Cookies ab, betrifft jedoch nicht nur diese.

5.2.1.1 Hinweise zu Nutzungsbeginn und jederzeit

Jeder Anbieter von Telemedien ist nach § 13 Abs.1 TMG dafür verantwortlich, dass sich der Nutzer zu Beginn des Nutzungsvorgangs und jederzeit über den Umgang mit seinen personenbezogenen Daten und die Erhebung und Verwendung in einem automatisierten Verfahren, welches die Verwendung personenbezogener Daten vorbereitet, informieren kann. Aus dieser Anforderung er-

[13] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 28 BDSG, Rn. 17 ff.

wächst die Verpflichtung, die Datenschutzhinweise derart zu verankern, dass der Nutzer zwangsläufig und so frühzeitig wie möglich mit diesen in Berührung gelangt. Deshalb muss die Information in einer Erklärung, die als „Datenschutzerklärung", „Hinweise zum Datenschutz" o.ä. bezeichnet und ohne Umwege erreichbar ist, erfolgen. Eine Information, die im Impressum oder den Allgemeinen Geschäftsbedingungen (AGB) erfolgt, genügt nicht den Anforderungen an die Transparenz. Die Datenschutzhinweise müssen sich auf den konkret und aktuell angebotenen Dienst beziehen. Nicht ausreichend ist es, wenn gesetzliche Normen wiedergegeben oder allgemeine Floskeln zur Wichtigkeit des Datenschutzrechts angezeigt werden. Auch sind zukünftig geplante oder ggf. in anderen Staaten stattfindende Datenumgänge nicht abstrakt in den Informationen darzustellen. Selbst wenn die Ausführungen entsprechend gekennzeichnet sind, wirkt dies der erforderlichen allgemeinen inhaltlichen Verständlichkeit entgegen. Die Information muss den gegenwärtigen Zustand abbilden und für den Nutzer relevant sein (d.h. keine allgemeine Darstellung der Praxis in anderen Rechtsordnungen auf der obersten Ebene). Soweit ein Dienst Änderungen erfährt, die dazu führen, dass weitere, andere oder weniger personenbezogene Daten erhoben und verwendet werden, ist die Datenschutzerklärung zu aktualisieren, so dass der Nutzer weiterhin über den konkreten und aktuellen Datenumgang bei der Nutzung des Dienstes informiert wird.

Zu beachten ist insbesondere auch, dass nicht sonstige Textbausteine, die häufig für herkömmliche Webseiten erstellt werden, genutzt werden, da eine Abweichung zwischen Smart-TV-Diensten und herkömmlichen Webseiten bei den Einstellungsmöglichkeiten für den Nutzer besteht. Während bei gängigen Internetbrowsern gezielt Einstellungen zur Privatsphäre und zum Datenschutz vorgenommen werden können, wie z. B. das Löschen von Tracking-Cookies, ist es dem Nutzer bei Smart-TV-Geräten über Betriebssystemmittel regelmäßig noch nicht möglich, derartige Maßnahmen zu ergreifen. Werden diese allerdings in der Datenschutzerklärung unter Bezugnahme auf die Webseite dargestellt, so ist dies irreführend, weil sie auf die Nutzung des konkreten Angebots keine Anwendung finden.

5.2.1.2 Kontaktmöglichkeiten

Um dem Nutzer die unkomplizierte Wahrnehmung seiner Nutzerrechte zu ermöglichen, sollten Anbieter eine einfache Kontaktmöglichkeit (z.B. postalische Adresse, E-Mail Adresse) zu ihnen bzw. einer bei ihnen für datenschutzrechtliche Fragen zuständigen Stelle in der Datenschutzerklärung angeben.[14] Dies ist insbesondere dann hilfreich, wenn mehrere Anbieter an der Erbringung von Diensten beteiligt sind und dem Nutzer nicht ohne weiteres ersichtlich ist, welche Stelle für welche Datenverarbeitungsvorgänge verantwortlich ist. Dies kann sich regelmäßig gerade erst aus der transparenten Darstellung in der Datenschutzerklärung ergeben.

[14] Zwar kann aus dem Impressum gem. §§ 5 f. TMG entnommen werden, wer Diensteanbieter ist, empfehlenswert ist es jedoch, wenn darüber hinaus ein Kontakt für datenschutzrechtliche Fragestellungen in der Datenschutzerklärung angegeben wird.

5.2.2 Unterrichtungspflicht der verantwortlichen Stelle

Gem. § 4 Abs. 3 Satz 1 BDSG ist die betroffene Person, bei der personenbezogene Daten erhoben werden, von der verantwortlichen Stelle grundsätzlich über die Identität der verantwortlichen Stelle (Nr. 1), die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung (Nr. 2) und die Kategorien von Empfängern zu informieren. Werden personenbezogene Daten ohne Kenntnis des Nutzers zu eigenen Zwecken gespeichert, ist der Nutzer grundsätzlich über die Speicherung, die Art der Daten, die Zweckbestimmung des Datenumgangs und die Identität der verantwortlichen Stelle zu benachrichtigen (vgl. § 33 BDSG). Soweit eine verantwortliche Stelle zugleich Diensteanbieter ist, kann die Information im Rahmen der Datenschutzerklärung gegeben werden, ansonsten bedarf es einer sonstigen Information des Nutzers. Sinn und Zweck der Information ist, dass sich ein Nutzer frei entscheiden können muss, ob er mit dem Datenumgang einverstanden ist. Hieraus folgt, dass die Information bereits vor der Erhebung, Verarbeitung und Nutzung erfolgen muss.

5.3 Nutzerrechte

Jeder Nutzer, dessen personenbezogene Daten erhoben und verwendet werden, hat gem. § 34 BDSG (ggf. i. V. m. § 13 Abs. 7 TMG) das Recht, Auskunft über die durch die verantwortliche Stelle zu seiner Person gespeicherten Daten zu verlangen. Gemäß § 35 BDSG kann er die Berichtigung, Löschung und Sperrung von Daten verlangen. Diese Ansprüche bestehen auch bei Nutzung eines Smart-TV-Angebotes. Smart-TV-Diensteanbieter sollten deshalb wie sonstige verantwortliche Stellen bei der Verarbeitung von Nutzerdaten (Bestands-, Nutzungs- und Inhaltsdaten) auf entsprechende Anfragen von Nutzern vorbereitet sein, um bei Bedarf zeitnah reagieren zu können. Wenn ein Anbieter seiner Auskunftspflicht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, kann dies mit einem Bußgeld geahndet werden.

5.4 Datenschutzrechtliche Grundsätze

Selbstverständlich gelten im Zusammenhang mit dem Angebot von Smart-TV-Diensten die sich aus den Vorschriften des BDSG und auch des TMG ergebenden datenschutzrechtlichen Grundsätze. Hierzu zählen u.a.:

5.4.1 Grundsatz der Direkterhebung

Gem. § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Ausnahmen bestehen nach § 4 Abs. 2 Satz 2 BDSG nur dann, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder wenn die Erhebung beim Nutzer einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte für die Beeinträchtigung eines überwiegend schutzwürdigen Interesses des Nutzers besteht. Der Nutzer soll wissen, wer welche Daten zu welchen Zwecken über ihn erhebt, verarbeitet und nutzt. Die personenbezogenen Daten müssen somit nicht nur bei ihm direkt, sondern auch mit seiner Kenntnis oder unter seiner Mitwirkung er-

langt werden. Findet eine Datenerhebung heimlich statt, so wird der Grundsatz der Direkterhebung verletzt, soweit nicht eine der im Gesetz genannten Ausnahmen greift.

Im Rahmen eines Online-Angebotes ist es daher notwendig, den Nutzer konkret über die Erhebung und Verwendung seiner personenbezogenen Daten zu informieren (vgl. 5.2) und die gegebenenfalls erforderliche Einwilligung einzuholen.

5.4.2 Grundsatz der Datenvermeidung und der Datensparsamkeit

Nach den in § 3a BDSG normierten Grundsätzen der Datenvermeidung und Datensparsamkeit sollten so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden.

Diese Grundsätze sind bereits frühzeitig, möglichst bei der Entwicklung eines Verfahrens oder Diensteangebots zu beachten. Die Angebote sind daher so zu entwickeln und zu betreiben, dass von Beginn an so wenig personenbezogene Daten wie möglich erhoben und verwendet werden („Privacy by design“) und standardmäßig die datenschutzfreundlichste Voreinstellung vorgenommen wird („Privacy by default“).

Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit den Anbietern von Smart-TV-Diensten dürfen deshalb erst stattfinden, wenn diese durch die Nutzer selbst initiiert werden, er also einen Dienst in Anspruch nehmen möchte und deshalb die Daten überhaupt benötigt werden. Ohne eine Inanspruchnahme durch den Nutzer bedarf es keines Datenumganges. Die Datenerhebung und -verwendung kann somit vermieden werden (konkret im Zusammenhang mit HbbTV-Angeboten, vgl. Kapitel 7.2).

Auch wenn die verantwortliche Stelle auf die Implementierung datenschutzfreundlicher Voreinstellungen hinzuwirken hat, ist es wünschenswert, dass Entwickler von Verfahren und Produkten diese bereits so herstellen, dass Datenflüsse nicht ohne weiteres ausgelöst werden.

Das Gebot der Datensparsamkeit und der Datenvermeidung verlangt z.B., dass Gerätehersteller Funktionalitäten wie Mikrofon (für Spracherkennung) und Kamera (für Gestensteuerung) so einbinden müssen, dass diese erst durch den Nutzer aktiviert werden und darüber hinaus, dass auf dem Gerät gespeicherte Daten der Kontrolle der Nutzer unterliegen, also z.B. Cookies verwaltet werden können[15].

5.4.3 Grundsatz der Zweckbindung

Jeder Umgang mit personenbezogenen Daten muss einen bestimmten, legitimen Zweck verfolgen. Eine Datensammlung ohne einen konkret festgelegten Zweck ist genauso wenig zulässig wie die

[15] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 3

Änderung eines früher festgelegten Zwecks und Verwendung der bis dahin gesammelten Daten für einen neuen Zweck, ohne dass auch für diesen Datenumgang eine Erlaubnis existiert. Soweit der verfolgte Zweck wegfällt, sind die personenbezogenen Daten grundsätzlich zu löschen. Im Falle gesetzlicher Verpflichtungen zur weiteren Aufbewahrung (etwa nach Vorgaben der Abgabenordnung oder des Handelsgesetzbuches) sind die Daten zu sperren und dazu von den aktuellen Produktivdaten zu trennen.

5.4.4 Grundsatz der Erforderlichkeit

Der Grundsatz der Erforderlichkeit bedeutet, dass nur die für einen konkreten Zweck erforderlichen personenbezogenen Daten erhoben und verwendet werden dürfen. Sofern Möglichkeiten bestehen, personenbezogene Daten durch Verarbeitungsschritte so zu verändern, dass der Informationsgehalt auf das erforderliche Mindestmaß begrenzt wird, sind diese umzusetzen.

5.4.5 Grundsatz der anonymen und pseudonymen Nutzung

Soweit es dem Diensteanbieter technisch möglich und zumutbar ist, hat er die Nutzung von Telemedien und ihre Bezahlung gem. § 13 Abs. 6 TMG anonym oder unter Pseudonym zu ermöglichen. Über diese Möglichkeit ist der Nutzer zu informieren. Dem Nutzenden muss z.B. bei Apps zur Nutzung sozialer Netzwerke jedenfalls die Möglichkeit gegeben werden, unter einem Pseudonym zu agieren.

6. Technische und organisatorische Maßnahmen

Zusätzlich zu den in den vorigen Kapiteln genannten datenschutzrechtlichen Anforderungen haben die Anbieter von Smart-TV-Diensten die technischen und organisatorischen Anforderungen, die sich aus § 9 BDSG und der Anlage zu § 9 BDSG sowie aus § 13 Abs. 4 TMG ergeben, einzuhalten. Insbesondere betrifft dies die folgenden Anforderungen:

6.1 Regelmäßige Sicherheitsupdates

Die verantwortlichen Stellen für die Smart-TV-Geräte müssen dafür Sorge tragen, dass regelmäßige Sicherheitsupdates angeboten werden. Stehen für ein (älteres) Gerät keine Patches mehr zur Verfügung, sollte dies dem Nutzer bei Einschalten des Gerätes bzw. vor Nutzung eines Dienstes mitgeteilt werden. Die Updates müssen auch Komponenten von Drittanbietern, die durch die verantwortliche Stelle genutzt werden, umfassen (z.B. Browser-Engine, Bibliothek für Videowiedergabe,…).

6.2 IT-Sicherheitsarchitektur

Bei Smart-TVs besteht, wie bei anderen mit dem Internet verbundenen Geräten (PCs, Smartphones,…) auch, die Gefahr, dass einzelne Anwendungen (App, Webseite, HbbTV-Seite) oder Medien

(MP3, Filme) durch Unbefugte derart manipuliert werden, dass diese einen Zugriff auf andere Bereiche des Gerätes (z.B. Kamera, Mikrophon, Cookie-Datenbank, Passwörter, DNS-Einstellungen,…) erlangen. Aus diesem Grund ist es notwendig, dass geeignete IT-Sicherheitsarchitekturen Anwendung finden, beispielsweise unterschiedliche Benutzerrechte auf Systemebene für einzelne Anwendungen oder Sandboxing-Verfahren.

6.3 Verschlüsselung nach dem Stand der Technik

Bei Nutzung des Smart-TV werden sämtliche Inhalte, wie z.B. Geräteupdates, Grafiken, Nachrichten, HbbTV-Inhalte oder Empfehlungsdienste meist über das HTTP-Protokoll übertragen. Werden dabei auch personenbezogene Daten übertragen, müssen diese nach dem Stand der Technik verschlüsselt werden (Anlage zu § 9 BDSG). Als Orientierung können die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) herangezogen werden. Zum Zeitpunkt der Erstellung der Orientierungshilfe sind aber mindestens folgende Anforderungen umzusetzen:

- HTTPS
- Perfect Forward Secrecy
- kein SSL2/SSL3
- mindestens 2048-Bit beim X.509 Zertifikat
- keine RC4-Verschlüsselung
- kein SHA1-Hashverfahren

Darüber hinaus müssen vorhandene Sicherheitsprobleme, die sich aus der Implementierung des TLS-Protokolls ergeben können, zeitnah durch Updates behoben werden (z.B. Heartbleed-Lücke).

Die Smart-TV-Hersteller müssen die HTTPS-Verschlüsselung derart implementieren, dass keine Man-In-The-Middle Attacken durch ungenügende Prüfung Serverzertifikate möglich sind.

7. Konkrete Anforderungen an Anbieter von Smart-TV-Diensten

Adressat datenschutzrechtlicher Vorgaben für den Umgang mit personenbezogenen Daten und somit verantwortlich für die Umsetzung der datenschutzrechtlichen Anforderungen ist jeweils der Diensteanbieter bzw. die verantwortliche Stelle. Um die datenschutzrechtlichen Verantwortlichkeiten auseinanderhalten zu können, ist strikt zwischen den verschiedenen Anbietern von Smart-TV-Diensten und deren jeweiliger Verantwortlichkeit zu unterscheiden. Nur auf diese Weise können die Rechte und Pflichten der einzelnen Anbieter bestimmt werden.

Im Folgenden werden die einzelnen Akteure nochmals (vgl. bereits Kapitel 3) benannt und die gesetzlichen Anforderungen („muss“) und Empfehlungen („sollte“) der Aufsichtsbehörden bezogen auf den jeweiligen Akteur dargestellt. Da dies jedoch nur schematisch geschehen kann, wird darauf hingewiesen, dass die Darstellung der rechtlichen Pflichten und Empfehlungen nicht abschließend ist. Soweit ein Ak-

teur mehrere Funktionen wahrnimmt (z.B. Gerätehersteller ist auch Portalbetreiber) muss er die Vorgaben und Empfehlungen der entsprechenden Abschnitte kumuliert beachten.

7.1 Gerätehersteller

Wie bereits unter Kapitel 3.1 dargestellt, agiert ein Gerätehersteller, der lediglich das Gerät und ggf. Software-Updates zur Verfügung stellt, dann als verantwortliche Stelle, wenn er im Rahmen der Software-Updates personenbezogene Daten, wie z.B. die IP-Adresse erhebt und verwendet. Bietet der Gerätehersteller Telemediendienste an, so agiert er als Telemedienanbieter, womit er den datenschutzrechtlichen Vorgaben des TMG unterliegt.

7.1.1 Information des Nutzers

Der Gerätehersteller muss den Nutzer über den Umgang mit dessen personenbezogenen Daten informieren. Die Informationspflicht der verantwortlichen Stelle erwächst i.d.R. aus § 4 Abs.3 BDSG (vgl. Kapitel 5.2.2.1). Im Rahmen dieser Information sollte der Nutzer auch darüber informiert werden, wann er das Angebot des Geräteherstellers verlässt und damit Nutzerdaten durch eine andere verantwortliche Stelle erhoben werden. Dabei wird jedoch nicht gefordert, dass vor jeder Weiterleitung ein Pop-Up erscheint; vielmehr genügt eine einmalige, aktive Information des Nutzers (z.B. bei der Einrichtung des Gerätes), die jederzeit aktiv durch den Nutzer wieder aufgerufen werden kann. Dies kann z.B. der Fall sein, wenn der Portalbetreiber nicht mit dem Gerätehersteller identisch ist. Zwar muss der Portalbetreiber den Nutzer über seine Identität und den Datenumgang informieren (vgl. Kapitel 7.3.2). Durch den Hinweis seitens des Geräteherstellers wird der Nutzer jedoch bereits im Vorfeld darauf hingewiesen, dass er im Begriff ist, das Angebot des Geräteherstellers zu verlassen. Der Nutzer kann sich bereits, bevor personenbezogene Daten durch den Portalbetreiber erhoben werden, für oder gegen eine Nutzung durch den Portalbetreiber entscheiden.

Soweit der Gerätehersteller selbst zugleich Anbieter von Telemedien ist, ist er verpflichtet, den Nutzer im Rahmen einer Datenschutzerklärung gem. § 13 Abs.1 TMG über Art, Umfang und Zweck des Datenumgangs zu informieren (vgl. Kapitel 5.2.1). Zudem muss dem Nutzer dann die Weitervermittlung zu einem anderen Anbieter angezeigt werden (vgl. § 13 Abs. 5 TMG).

7.1.2 Software-Update

Hinsichtlich eines möglichen Software-Updates ist der Nutzer bei der Einrichtung des Gerätes durch eine Information (welche in der Firmware enthalten ist) darauf hinzuweisen, dass regelmäßig neue Software-Updates durch den Gerätehersteller zur Verfügung gestellt werden. Der Nutzer sollte gebeten werden, auszuwählen, ob er

1. manuell die Prüfung und Installation neuer Updates durchführen möchte,
2. automatisch neue Updates ohne Interaktion installieren möchte oder
3. eine Benachrichtigung wünscht, sobald ein neues Update zur Verfügung gestellt wird.

Entscheidet sich der Nutzer für die Option 1., liegt es in seiner Sphäre, wann er eine Überprüfung anstößt, ob ein Software-Update zur Verfügung steht und damit Datenflüsse (z.B. IP-Adresse) auslöst. Bei den Optionen 2. und 3. hingegen findet in regelmäßigen Abständen ein Abruf des aktuell installierten Softwarestandes statt. Ist eine aktuellere Software verfügbar, wird diese dann automatisch oder nach Bestätigung des Nutzers installiert. In allen drei Fällen sollte der Nutzer über die Datenflüsse und die Neuerungen, die mit einem Update einhergehen werden (Option 1. und 3.) bzw. einher gingen (Option 2), wie z. B. Aktualisierung der Software oder Schließen von Sicherheitslücken, informiert werden.

Soweit personenbezogene Daten für die Abfrage des Software-Standes, die Zusendung von Informationen und das Einspielen des Software-Updates erforderlich sind, dürfen diese im gesetzlich erlaubten Umfang erhoben und verwendet werden.

7.1.3 Analyse des Nutzerverhaltens

Einige Gerätehersteller analysieren das Verhalten der Nutzer bei der Bedienung, aber auch bei der Einrichtung des Gerätes, um z.B. die Menü-Führung bei der Einrichtung des Gerätes verbessern zu können. Da bei einer solchen Analyse zumindest die IP-Adresse an den Gerätehersteller fließt, bedarf es einer Erlaubnis für die Erhebung und ggf. Verwendung der personenbezogenen Daten. Eine Erlaubnis aus dem Gesetz ist jedoch nicht ersichtlich, so dass es einer Einwilligung des Nutzers bedarf, um das Nutzerverhalten erheben und analysieren zu dürfen.

7.1.4 Umgang mit Gerätekennungen

7.1.4.1 Erheben und Nutzen von Gerätekennungen

Erhebt und verwendet der Gerätehersteller eindeutige Gerätekennungen, bedarf er hierfür entweder einer Erlaubnis aus dem Gesetz oder einer Einwilligung des Nutzers (vgl. Ziffer 5.1). Für die Einstufung einer eindeutigen Gerätekennung als personenbezogenes Datum spielt es zunächst keine Rolle, ob Gerätekennungen fest lokal auf dem Gerät hinterlegt sind (z.B. MAC-Adresse, Seriennummer) oder durch den Hersteller bei einem erstmaligem Start des Gerätes vergeben werden (z.B. im Rahmen von Cloud-Diensten) – vielmehr muss eine Person bestimmbar sein (vgl. hierzu Kapitel 2.4). Ob und welche Rechtsgrundlage im Einzelfall greift, hängt von dem konkreten Zweck ab, zu dem die Gerätekennung benötigt wird. Ist die Erhebung und Verwendung einer eindeutigen Gerätekennung nicht erforderlich, sondern werden hierdurch z.B. lediglich künftige Servicedienste durch eine erleichterte nachträgliche Zusammenführung von Gerätedaten mit einem

konkreten Nutzer möglich, ist eine Erforderlichkeit zunächst[16] nicht erkennbar und es bedarf einer Einwilligung des Nutzers.

7.1.4.2 Deaktivierung von Schnittstellen

Der HbbTV-Standard definiert eine minimale Unterstützung von verschiedenen Standards, die für ein einheitliches Funktionieren von HbbTV-Inhalten sorgen sollen. Ein expliziter Zugriff auf eindeutige Gerätekennungen ist nicht Teil des Standards. Da diese von Seiten der HbbTV-Anbieter aber möglicherweise zur Realisierung von gerätebezogenen Trackingverfahren verwendet werden könnten, sollte ein Hersteller den Zugriff (evtl. auch bei Verwendung von Drittanbieterbibliotheken) auf diese Schnittstellen überprüfen und eindeutige Gerätekennungen mit einem leeren Wert (Nullstring) ersetzen. So sollte beispielsweise sichergestellt sein, dass die Implementierung einer der HbbTV-Standards, der OIPF, „Volume 5 - Declarative Application Environment“ einen Zugriff über die Netzwerkschnittstelle auf die MAC-Adresse nicht umsetzt.

7.1.5 Verwaltung von Cookies

Wie im „klassischen“ Internet werden für die Realisierung von HbbTV-Inhalten häufig Cookies eingesetzt. Diese können es technisch ermöglichen, eine eindeutige Kennung auf dem Smart-TV des HbbTV-Nutzers abzulegen. Aus diesem Grund sollten[17] bei Smart-TV-Geräten, so wie bei den meisten Browsern auf PCs auch, Standardfunktionalitäten zur Verwaltung von Cookies vorhanden sein:

1. Anzeige aller Cookies, die von den HbbTV-Anbietern (und Dritten, die in den HbbTV-Seiten eingebunden sind) gesetzt werden
2. Grundsätzliches Blockieren von Cookies, insbesondere von Dritten, sogenannten Third-Party-Cookies, da damit ein webseitenübergreifendes Tracking möglich ist.
3. Möglichkeit zum Löschen aller Cookies eines HbbTV-Angebots bei Wechsel des Senders oder bei Ausschalten des Gerätes (auch auf Standby).

Zusätzlich zu den „klassischen“ Cookies, den sogenannten HTTP-Cookies, ist es bei Verwendung von HTML5 auch möglich, dessen Speichertechniken als Cookie-Ersatz zu gebrauchen. Es soll dem Nutzer möglich sein, diese Art der Cookies genauso wie die HTTP-Cookies zu verwalten (Anzeige, Verhinderung, Löschung).

---

[16] Selbst wenn eine Erforderlichkeit für die Wiedererkennung eines Gerätes für die inhaltliche Ausgestaltung des Vertragsverhältnisses besteht, ist dazu regelmäßig nicht zwingend die eindeutige Geräteerkennung erforderlich; vielmehr kann ein sonstiges, zufällig vergebenes Identifizierungsmerkmal verwendet werden.

[17] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 3

7.1.6 Red Button ohne Autostart-Funktion

Ist eine HbbTV-URL im linearen Rundfunksignal vorhanden, wird die darin referenzierte HbbTV-Seite automatisch über das Internet geladen. Diese Art der Autostartfunktion wird bei den meisten HbbTV-Inhalten eingesetzt. Einige wenige Gerätehersteller bieten jedoch ihre Geräte bereits (von vornherein bzw. nachdem ein Nutzer dies aktiv in den Einstellungen auswählt) derart an, dass vor dem Laden von HbbTV-Angeboten und der damit einhergehenden wechselseitigen Kommunikation zunächst nur eine Information erscheint, dass ein solches Angebot verfügbar ist. Erst wenn der Nutzer aktiv den Red Button klickt, wird eine Internetverbindung aufgebaut und das jeweilige Angebot geladen. Mit einem zweiten Aktivieren des Red Button gelangt der Nutzer dann in das jeweilige HbbTV-Angebot. Zudem stellen einige Gerätehersteller die Auswahl der HbbTV-Angebote zur Disposition, d.h. der Nutzer selbst kann senderbezogen im Menü auswählen, welche konkreten HbbTV-Angebote ihn interessieren und ggf. automatisch geladen werden sollen und bei welchen nicht einmal eine Verfügbarkeits-Information über das vorhandene Angebot erfolgen soll. Auch wenn diesbezüglich derzeit keine datenschutzrechtliche Verantwortung der Gerätehersteller besteht, den Datenfluss zu unterbinden, sind diese Voreinstellungen bzw. Einstellungsmöglichkeiten vor dem Hintergrund des Grundsatzes der Datenvermeidung und der Datensparsamkeit besonders positiv hervorzuheben. Da diese datenschutzfreundliche Funktion noch nicht Bestandteil des HbbTV-Standards ist, sollte diese bei einer zukünftigen Erweiterung mit hinzugenommen werden.

Die Gerätehersteller sollten es deshalb als Option für den Nutzer ermöglichen, dass bei Erkennen eines HbbTV-Inhaltes im linearen Signal z.B. ein standarisierter Red Button bzw. anderweitiges Zeichen eingeblendet wird, das unabhängig von der HbbTV-Seite ist und nicht über das Internet geladen wird. Erst nach Information der Nutzer über die Bedeutung dieses Zeichens und nach aktivem Drücken des Red Buttons sollte die HbbTV-Seite, die dann senderspezifisch ist, über das Internet geladen werden. Diese Funktion entspricht einem Privacy-by-Design-Ansatz und sollte als Voreinstellung aktiv sein (Privacy-by-Default), soweit Hersteller bzw. Programmanbieter eine entsprechend Funktionalität nicht durch andere, ebenso wirksame Maßnahmen sicherstellen.

7.1.7 Technische Prüftransparenz

Eine starke Verschlüsselung ist für die Wahrung der Vertraulichkeit und Integrität der bei Smart-TV übermittelten Daten sinnvoll und für personenbezogene Daten zwingend notwendig. Zur Überprüfung der übertragenen Inhalte eines Smart-TV-Gerätes sollten aber sichere Mechanismen zur Verfügung gestellt werden, die Prüfern und technisch interessierten Nutzern einen Einblick in die eigenen Daten des eigenen Smart-TV-Gerätes innerhalb des eigenen (Labor-)Netzes an die beteiligten Server ermöglichen. Diesbezüglich wären mehrere technische Verfahren möglich:

- Es könnte, wie es bei Smartphones üblich ist, für einen Smart-TV-Nutzer möglich sein, dass eigene selbstsignierte **Zertifikate** dem Gerät bekannt gemacht werden (z.B. über USB-Stick im Servicemenü). Sollte dies von einem Gerätehersteller aus Sicherheitsgründen nicht gewünscht sein, so wäre auch eine Erzeugung des selbstsignierten Serverzertifikate des eigenen Smart-TV durch das eigene Gerät vorstellbar, dass vom Smart-TV auf einen Analyserechner herunterge-

laden werden kann. Dieser Vorgang könnte in Laborumgebungen, die von Fachmedien, interessierten Nutzern, der IT-Sicherheitsforschung, den Verbraucherschützern und Datenschutzaufsichtsbehörden durchgeführten Man-In-The-Middle-Analysen im eigenen Netz in die Lage versetzen, eine technische Prüftransparenz der eigenen Smart-TV-Daten herzustellen. Erhöhte Sicherheitsrisiken erstehen durch dieses Verfahren kaum, da nur der HTTPS-Datenverkehr des eigenen Testgeräts entschlüsselt werden kann. Sollten sicherheitsrelevante Informationen (z.B. Authentifizierungstokens des Backends) Bestandteil des Datenverkehrs sein, könnten diese durch eine zusätzliche Verschlüsselung geschützt werden.

- Eine vorinstallierte Anwendung des Smart-TV-Herstellers, die als **Netzwerkmonitor**[18] fungiert, könnte einem Nutzer nach Aktivierung alle http-basierten Internetverbindungen seines Smart-TV-Gerätes mit Dritten anzeigen. Für jeden Aufruf müsste dann ein Zeitstempel, der Empfangsserver (IP-Adresse und Domainname), der http-Header sowie HTTP-Requests und HTTP-Responses anzeigt werden. Auch Inhalte von HTTPS-Verbindungen könnten so dargestellt werden, da der Netzwerkmonitor die eigenen Daten auf dem eigenen Gerät vor der Verschlüsselung darstellt.

7.1.8 Umgang mit Kameras und Mikrofonen

Enthält ein Smart-TV-Gerät Kameras oder Mikrofone, besteht ein besonderes Risiko, dass im Falle eines unbefugten Zugriffs auf diese Gerätebestandteile der Nutzer in seiner Privat- oder sogar Intimsphäre verletzt wird. Aus diesem Grund sollen besondere Sicherheitsmechanismen vorhanden sein, die das Missbrauchsrisiko deutlich minimieren oder Missbrauch zumindest aufdecken:

- Es sollte möglich sein, die Nutzung von Kameras und Mikrofonen über eine Geräteeinstellung dauerhaft abzuschalten.
- Vor Installation bzw. Start von Anwendungen, die Zugriff auf Kameras oder Mikrofone einfordern, sollte die Zustimmung des Nutzers eingeholt werden.
- Es sollte über ein Gerätemenü möglich sein, die Liste der Anwendungen, die Zugriff auf Kameras oder Mikrofone haben, zu verwalten.
- Bei aktiver Aufnahme sollte der Nutzer über ein visuelles Symbol darüber informiert werden, z.B. durch ein gut sichtbares LED-Signal neben der Kameralinse oder dem Mikrofonausschnitt. Hinweissignale müssen derart aktiviert werden, dass sie von einer kompromittierten Anwendung nicht ausgeschaltet werden können (z.B. über „Verdrahtung“ auf Hardwareebene).
- Vertrauensfördernd für den Nutzer wäre die Bereitstellung von Möglichkeiten, kritische Bereiche wie Kameralinse oder Mikrofonausschnitt mechanisch zu deaktivieren oder abzudecken, z.B. mit einer verschiebbaren Klappe. Solche klar erkennbaren Schutzvorrichtungen können durch Software-Manipulation nicht überlistet werden und Nutzern so das ggf. unbestimmte

[18] Im Jahr 2015 bietet zum Beispiel der Browser Firefox die „Netzwerkanalyse“ für eine dynamische Analyse von Web-Content an.

Gefühl des Beobachtet oder Belauschtwerdens nehmen. Versehen z.B. mit dem Hersteller-Logo könnten Abdeckungen sogar als prägendes Design-Element für ein Smart-TV-Gerät ausgestaltet werden.

7.2 HbbTV-Anbieter

7.2.1 Zulässiger Datenumgang

Wird eine HbbTV-URL mit dem Rundfunksignal versandt und die entsprechende Seite unmittelbar und ohne Tätigwerden des Nutzers von dem Server des HbbTV-Anbieters unter Eröffnung eines Rückkanals für die Übertragung von Online-Inhalten, bei denen zumindest[19] - technisch bedingt - das personenbezogene Datum IP-Adresse übertragen und verwendet wird, abgerufen, so ist für diesen Datenverarbeitungsschritt eine Rechtsgrundlage nicht erkennbar.

Weder willigt der Nutzer in diesen Datenumgang ein, noch ist eine Erlaubnis aus dem Gesetz einschlägig. Insbesondere kann § 15 Abs. 1 TMG nicht greifen, da allein aufgrund der Nutzung eines Smart-TV-Gerätes und dem Einschalten eines Senders, der HbbTV-Inhalte anbietet, noch nicht von der „Inanspruchnahme von Telemedien“ im Sinne des § 15 Abs. 1 TMG durch den Fernsehzuschauer und damit noch nicht von einem Anbieter-Nutzer-Verhältnis ausgegangen werden kann.[20] Ein solches ist jedoch für die Eröffnung des Anwendungsbereichs des Telemediengesetzes elementar. So spricht z.B. § 11 Abs. 2 TMG davon, dass Nutzer jede natürliche Person ist, die Telemedien nutzt, und § 14 Abs. 1 stellt auf die Begründung eines Vertragsverhältnisses ab. Daher genügt als Voraussetzung für die Anwendbarkeit des § 15 Abs. 1 TMG weder die Einrichtung eines Internetanschlusses noch die Herstellung einer Verbindung mit dem Internet, sondern es ist ein aktives Aufrufen des Telemediendienstes erforderlich.

Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit den Anbietern von Smart-TV-Diensten dürfen deshalb erst stattfinden, wenn diese durch die Nutzer selbst initiiert werden, z.B. durch die aktive Entscheidung, den Red-Button bei HbbTV zu aktivieren und damit den Abruf eines Telemediendienstes bewusst zu veranlassen. Dies könnte durch eine Auswahl der HBBTV-Fernsehsender in einem Menü des Smart-TV oder durch ein Opt-In-Cookie des HBBTV-Angebots, das durch auf eine mit dem lineare Karusselverfahren ausgelieferte HBBTV-Startseite ausgewertet wird, realisiert werden. Das bloße Verbinden des Gerätes mit dem Internet ist dagegen nicht als bewusste Inanspruchnahme von Telemedien zu bewerten, da dies nicht zwingend dahingehend verstanden werden kann, dass eine Nutzung des HbbTV-Angebotes beim Empfang des Fernsehprogramms ohne weiteren Zwischenschritt gewünscht ist. Eine Erlaubnis für die Erhebung der IP-Adresse bzw. weiterer Nutzungsdaten ist dann nicht gegeben. Die standardmäßi-

[19] Im Rahmen einer Reichweitenmessung bzw. zum Zweck interessensbasierter Werbung könnten auch weitere Nutzungsdaten betroffen sein.

[20] Eine Rechtsgrundlage aus dem BDSG ist ebenfalls nicht ersichtlich.

ge Voreinstellung der HbbTV-Nutzung und die damit zusammenhängende wechselseitige Kommunikation bei Einschalten des Gerätes und Auswahl eines Senders widersprechen dem.

HbbTV-Anbieter als für die Datenerhebung und -verwendung (zumindest der IP-Adresse) verantwortliche Stellen müssen Sorge dafür tragen, dass eine Kommunikation mit ihrem Server erst stattfindet, wenn der Nutzer aktiv den Red-Button auf seiner Fernbedienung drückt. Dies kann über das lineare Verfahren (auch Karussellverfahren genannt, siehe Kapitel 2.3) realisiert werden, bei dem die HbbTV-HTML-Startseite mittels des Rundfunksignals übertragen wird. In diesem Moment wird noch kein Rückkanal eröffnet. Erst bei der Aktivierung des Red-Buttons wird die volle Startseite aus dem Internet geladen und damit eine Internetverbindung aufgebaut

Sollte der HbbTV-Standard derart angepasst werden, dass ein Gerät so eingestellt werden kann, dass die HbbTV-Startseite erst nach Drücken des Red-Buttons geladen wird (siehe Kapitel 7.1.6), dann kann die HbbTV-Startseite auch über das Internet geladen werden.

Im Ergebnis müssen die HbbTV-Anbieter als verantwortliche Stellen, ggf. in Kooperation mit den Geräteherstellern es dem Nutzer ermöglichen, anonym - d.h. ohne dass personenbezogene Daten wie IP-Adressen und/oder Nutzungsdaten beim Einsatz von Verfahren zur Reichweitenmessung an den HbbTV-Anbieter fließen - fernsehen zu können.[21]

7.2.2 Datenschutzerklärung

Der HbbTV-Anbieter muss als Telemedienanbieter gem. § 13 Abs. 1 TMG eine Datenschutzerklärung vorhalten, die zu Beginn des Nutzungsvorganges und jederzeit auffindbar ist (vgl. Kapitel 5.2.1). Dass eine Datenschutzerklärung existiert und abrufbar ist, sollte dem Nutzer bereits über die Startseite deutlich gemacht werden. D.h., die über das Rundfunksignal ausgelieferte Startseite sollte bereits signalisieren, dass der Nutzer beim Aufruf des Vollbildes (Drücken des Red-Buttons) Zugang zu einer Datenschutzerklärung erhält. Diese Datenschutzerklärung muss im HbbTV-Angebot unmittelbar aufzufinden sein und auch jederzeit von jeder weiteren Seite aufgerufen werden können.

7.2.3 Nutzungsprofilbildung

Eine Nutzungsprofilbildung ist nur dann zulässig, wenn der Nutzer wirksam eingewilligt hat oder diese gem. § 15 Abs. 3 TMG zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Telemedienangebotes unter Pseudonym erfolgt und dem Nutzer eine wirksame Widerspruchsmöglichkeit angeboten wird (vgl. Kapitel 5.1.1.2). Über die Erstellung eines Nutzungsprofils und die Möglichkeit zu widersprechen, ist der Nutzer im Rahmen der Datenschutzerklärung (vgl. Kapitel 7.2.2) zu informieren.

[21] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smartem Datenschutz“ vom Mai 2014, Ziffer 1

Vor einem aktiven Aufruf des HbbTV-Angebotes ist auch die Erhebung von Nutzungsdaten zu Zwecken der Nutzungsprofilbildung nur auf der Grundlage einer informierten, ausdrücklichen und freiwilligen Einwilligung zulässig.

7.3 App-Store-Betreiber/ Portalbetreiber

7.3.1 Datenerhebung nur im erforderlichen Umfang

App-Store-Betreiber dürfen lediglich personenbezogene Daten erheben und verwenden, wenn hierfür eine Rechtsgrundlage oder eine Einwilligung des Nutzers gegeben ist. Grundsätzlich nicht erhoben werden dürfen daher Informationen darüber, welche App von welchem Nutzer installiert und gestartet wird, es sei denn, dies ist für die Durchführung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Verhältnisses zwischen dem Nutzer und dem App-Store-Betreiber bzw. für die Erbringung des Dienstes erforderlich. Regelmäßig nicht erforderlich ist die Erhebung von Geräte-IDs.

7.3.2 Datenschutzerklärung

Der App-Store Betreiber muss als Telemedienanbieter gem. § 13 Abs. 1 TMG eine Datenschutzerklärung vorhalten, die zu Beginn des Nutzungsvorganges und jederzeit auffindbar ist (vgl. Kapitel 5.2.1). Der Nutzer muss somit unmittelbar, nachdem er aktiv den App-Store aufgerufen hat, die Möglichkeit erhalten, sich über den Umgang mit seinen personenbezogenen Daten informieren zu können.

7.3.3 Nutzungsprofilbildung

Ein Nutzungsprofil unter Pseudonym zu Zwecken der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung des Telemediendienstes (App-Store) darf nur unter Einhaltung der Vorgaben des § 15 Abs. 3 TMG (vgl. Kapitel 5.1.1.2) erfolgen. Hierbei ist dem Nutzer eine wirksame Widerspruchsmöglichkeit und eine Information über die Nutzungsprofilbildung und die Möglichkeit, zu widersprechen, zur Verfügung zu stellen.

Geht eine Profilerstellung über den Anwendungsbereich des § 15 Abs. 3 TMG hinaus, bedarf es einer Einwilligung.

7.4 App-Anbieter

App-Anbieter unterliegen als Anbieter von Telemedien zahlreichen datenschutzrechtlichen Anforderungen, welche bereits in einer eigenen Orientierungshilfe, der „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ des Düsseldorfer Kreises vom 16.

Juni 2014 veröffentlicht wurden.[22] Auch wenn dort unter Kapitel 1 dargestellt wird, dass Besonderheiten von Apps, die für spezielle Endgeräte wie z.B. Smart-TVs entwickelt und angeboten werden, nicht berücksichtigt würden, kann das Dokument als Orientierung dienen. Besonderheiten bei Smart-TV-Apps sind jeweils im Einzelfall zu untersuchen und zu bewerten. Klassische Besonderheiten sind den Aufsichtsbehörden derzeit nicht bekannt.

7.5 Betreiber von Personalisierungsdiensten (Empfehlungsdienste)

7.5.1 Profilbildung für personalisiertes Angebot

Betreiber von Empfehlungsdiensten erheben regelmäßig Nutzungsdaten, um dem entsprechenden Nutzer Empfehlungen entsprechend seiner Interessen (Fernsehgewohnheiten, App-Nutzung) geben zu können. Nutzungsdaten dieser Dienste zu Empfehlungszwecken dürfen nur dann erhoben und verwendet werden, wenn die Voraussetzungen des § 15 Abs. 3 TMG eingehalten werden (vgl. Kapitel 5.1.1.2). Da derartige Nutzungsprofile gem. § 15 Abs. 3 Satz 3 und § 13 Abs. 4 Satz 1 Nr. 6 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden dürfen, ist eine Zusammenführung mit Registrierungsdaten, eindeutigen Geräte-IDs oder auch der IP-Adresse ohne Einwilligung des Nutzers unzulässig.

7.5.2 Anonyme oder pseudonyme Nutzung

Soweit sich ein Nutzer für einen Empfehlungsdienst registrieren kann, ist dem Nutzer gem. § 13 Abs. 6 TMG grundsätzlich eine Nutzung unter Pseudonym zu ermöglichen (vgl. Kapitel 5.4.5).

7.5.3 Datenschutzerklärung

Der Betreiber von Personalisierungsdiensten muss als Telemedienanbieter gem. § 13 Abs. 1 TMG eine Datenschutzerklärung vorhalten, die zu Beginn des Nutzungsvorganges und jederzeit leicht auffindbar ist (vgl. Kapitel 5.2.1).

7.6 Auftragsdatenverarbeiter

Auftragsdatenverarbeiter (vgl. Kapitel 2.1) können in die verschiedensten Datenumgänge eingebunden werden, indem ihnen bestimmte Datenverarbeitungs-Aufgaben übertragen werden. Der Auftragsdatenverarbeiter darf gem. § 11 Abs. 3 BDSG nur im Rahmen der Weisungen des Auftraggebers mit personenbezogenen Daten umgehen. Gem. § 11 Abs. 4 BDSG treffen den Auftragneh-

[22] Die „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ ist z.B. unter der URL http://www.lda.bayern.de/MobileApplikationen/index.html abrufbar.

mer nur bestimmte Verpflichtungen aus dem BDSG. Die Verantwortlichkeit für den Datenumgang im Rahmen der Auftragsdatenverarbeitung liegt jedoch bei dem Auftraggeber.

8 Handlungsmöglichkeiten und -verpflichtungen der Datenschutzaufsichtsbehörden

8.1 App-Anbieter

Datenschutzaufsichtsbehörden haben gemäß § 38 Abs. 1 Satz 2 BDSG die Aufgabe, verantwortliche Stellen mit Rücksicht auf deren typische Bedürfnisse zu beraten und zu unterstützen. Dies bedeutet, dass Anbieter von Smart-TV-Diensten sich von ihrer zuständigen Datenschutzaufsichtsbehörde u.a. dazu beraten lassen können, ob die Gestaltung ihres Beitrags zu der Smart-TV-Nutzung datenschutzkonform ist. Umfang und Intensität der Prüfung hängen dabei allerdings von den personellen Ressourcen und der Prioritätensetzung der Aufsichtsbehörde ab. Die Verantwortung bleibt bei den Diensteanbietern.

8.2 Anordnung nach § 38 Abs. 3 und 5 BDSG

Datenschutzaufsichtsbehörden haben gemäß § 38 Abs. 3 BDSG das Recht (und gelegentlich auch die Pflicht), von verantwortlichen Stellen und damit auch von Anbietern von Smart-TV-Diensten die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlichen Auskünfte, das heißt in diesem Zusammenhang insbesondere Auskünfte über die erhobenen personenbezogenen Daten der Smart-TV-Nutzer und die Verwendung dieser Daten, zu verlangen. Wenn Aufsichtsbehörden Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technische und organisatorische Mängel feststellen, können sie gemäß § 38 Abs. 5 BDSG Maßnahmen zur Beseitigung dieser Verstöße anordnen und bei schwerwiegenden Verstößen oder Mängeln die Nutzung oder den Einsatz einzelner Verfahren untersagen.

8.3 Bußgeldverfahren

Datenschutzrechtliche Bußgeldtatbestände sind insbesondere in § 16 TMG und § 43 BDSG enthalten. Verstöße können mit einer Geldbuße bis zu 50.000 Euro, zum Teil sogar bis zu 300.000 Euro geahndet werden.

So handeln Anbieter, die die nach § 38 Abs. 3 BDSG erbetene Auskunft vorsätzlich oder fahrlässig nicht, nicht vollständig oder nicht rechtzeitig erteilen, oder vollziehbaren Anordnungen zur Beseitigung festgestellter Verstöße oder der Untersagung der Nutzung oder des Einsatzes einzelner Verfahren nach § 38 Abs. 5 BDSG zuwiderhandeln, ordnungswidrig und können mit einem Bußgeld bestraft werden.

Anlage: Gemeinsame Position

Mai 2014

Gemeinsame Position
der

Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)

Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten

---

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von **Fernsehangeboten** muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als **Telemedien** den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und –verwendung informiert werden.
   - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z.B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
   - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV- Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.