Kommission für Jugendmedienschutz der Landesmedienanstalten

die medienanstalten

Gültig seit dem 10.09.2014

Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV

(„AVS-RASTER“)

Vorbemerkung

Die KJM legt hiermit aktuelle **Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme (AV-Systeme bzw. AVS) als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien** vor, die auf den gesetzlichen Vorgaben des Jugendmedienschutz-Staatsvertrags - § 4 Absatz 2 Satz 2 JMStV - beruhen. Gemäß den Jugendschutzrichtlinien der Landesmedienanstalten[1] ist Altersverifikation für geschlossene Benutzergruppen durch zwei miteinander verbundene Schritte sicherzustellen: erstens durch eine zumindest einmalige Identifizierung (Volljährigkeitsprüfung), die über persönlichen Kontakt erfolgen muss. Zweitens durch Authentifizierung beim einzelnen Nutzungsvorgang, um das Risiko einer Weitergabe von Zugangsberechtigungen an Minderjährige wirksam zu reduzieren. Dabei ist zwischen einer plausiblen Altersprüfung für den einmaligen Nutzungsvorgang (Stichwort: Einmalschlüssel) und einer verlässlichen Altersprüfung für den wiederholten Nutzungsvorgang (Stichwort: Generalschlüssel) zu unterscheiden. In beiden Fällen gilt, dass der Zugang zur geschlossenen Benutzergruppe

[1] erstellt durch die KJM, vom 08./09.03.2005; in Kraft getreten am 02.06.2005

grundsätzlich erst dann frei geschaltet werden darf, wenn das jeweilige Verfahren erfolgreich abgeschlossen ist. Eine vorherige Freischaltung des Zugangs (sog. „Schnupperzugang“) wird nicht akzeptiert.

Der JMStV enthält kein Anerkennungsverfahren für geschlossene Benutzergruppen oder AV-Systeme. Daher hat die KJM ein Verfahren der Positivbewertung entwickelt und bewertet auf Anfrage von Unternehmen oder Anbietern entsprechende Konzepte, bei Bedarf begleitet von Gesprächen oder Audits vor Ort. Dies dient der Verbesserung des Jugendschutzes im Internet und ist gleichzeitig ein Service für die Anbieter für mehr Rechts- und Planungssicherheit. Die Hauptverantwortung für die JMStV-konforme Gestaltung eines Internet-Angebots liegt aber beim Inhalte-Anbieter, nicht bei der KJM. Der Inhalte-Anbieter muss gemäß § 4 Abs. 2 S. 2 JMStV sicherstellen, dass pornografische und bestimmte andere jugendgefährdende Inhalte in seinem Angebot nur für Erwachsene zugänglich sind (geschlossene Benutzergruppen). Er kann sich dabei technischer Jugendschutz-Konzepte bedienen, die die KJM bereits positiv bewertet hat.

Davon bleiben aber zusätzliche Sicherungspflichten, wie **z.B. Backdoorschutz, zeitliche Begrenzung einer Sitzung, Time-Out nach bestimmter Idle-Time** usw. unberührt, die in KJM-Prüfverfahren überprüft werden können. Unberührt davon bleibt auch, dass der Inhalte-Anbieter sicherstellen muss, dass **keine absolut unzulässigen Inhalte nach § 4 Abs. 1 JMStV** in der geschlossenen Benutzergruppe zugänglich gemacht werden.

Mögliche Gegenstände für positive Bewertungen durch die KJM:

Die KJM bewertet sowohl Konzepte für Gesamtlösungen als auch für Teillösungen (Module) für geschlossene Benutzergruppen. Die Bewertung von Modulen ermöglicht Anbietern eine leichtere Umsetzung in der Praxis. So besteht für Anbieter die Möglichkeit, positiv bewertete Module im Baukastenprinzip zu Gesamtlösungen geschlossener Benutzergruppen zu kombinieren, die dann den Anforderungen des JMStV und der KJM entsprechen. Module können z.B. Verfahren nur für die Identifizierung bzw. die Authentifizierung oder andere wesentliche Bestandteile eines AV-Systems sein. Aber

auch ein AV-System ist letztlich nur ein Modul für eine geschlossene Benutzergruppe (wenn auch das Kernstück), da es nur die Funktion der „vorderen Eingangskontrolle“ zum geschlossenen Bereich erfüllt, für die Sicherstellung einer geschlossenen Benutzergruppe aber noch weitere Sicherungsmaßnahmen, wie Backdoorschutz etc. (s.o.), zu beachten sind.

Sollte ein Konzept je nach Ausgestaltung als AVS im Sinne des § 4 Abs. 2 S. 2 JMStV oder als technisches Mittel im Sinne des § 5 Abs. 3 Nr. 1 JMStV einsetzbar sein, ist eine Bewertung als „übergreifendes Jugendschutzkonzept“ möglich.

Die KJM **bewertet bislang ausschließlich Konzepte**. Für die aufsichtsrechtliche Beurteilung ist die Umsetzung der geschlossenen Benutzergruppen in der Praxis entscheidend.

Mit diesem **Bewertungsraster** für Konzepte für geschlossene Benutzergruppen sollen Entscheidungsprozesse der KJM bei der Bewertung transparent gemacht und Standards definiert werden. Das Raster orientiert sich am derzeitigen Stand der Technik. Es ist nicht abschließend und lässt eine Anpassung und weitere Verfeinerung der Kriterien jederzeit zu.

I. Konzepte der plausiblen Altersprüfung für den einmaligen Nutzungsvorgang (Stichwort: „Einmalschlüssel“)

Als Altersprüfung, die unmittelbar vor jeder Nutzung bzw. jedem Zutritt zu einer geschlossenen Benutzergruppe erneut durchgeführt wird („Einmalschlüssel“), ist z.B. die Nutzung der Altersbestätigung über die eID-Funktion des neuen Personalausweises denkbar.

Daneben können – vergleichbar mit der augenscheinlichen Kontrolle in einer Videothek –Verfahren ausreichend sein, die geeignet sind, die Volljährigkeit mit hoher Wahrscheinlichkeit (Plausibilitätsprüfung) festzustellen. Eine Plausibilitätsprüfung ist hier ausreichend, weil das gesamte Verfahren – anders als bei Konzepten der verlässlichen Altersprüfung für den wiederhol-

ten Nutzungsvorgang (s. hierzu unten Punkt II.) - bei jeder Nutzung durchlaufen werden muss.

Dies kann z.B. durch ein Verfahren gegeben sein, bei dem der Nutzer per Webcam in Augenschein genommen wird, sofern hierbei ausschließlich geschultes Personal zum Einsatz kommt, eine wirksame Lebenderkennung erfolgt und eine ausreichende Bildqualität gewährleistet ist. Lebenderkennung und ausreichende Bildqualität sind erforderlich, um sicherzustellen, dass es sich um eine echte Person handelt, die aktuell vor der Kamera sitzt und um Umgehungsmöglichkeiten beispielsweise mittels eingespielten Filmen oder Maskierung auszuschließen. Ist der Nutzer nicht zweifelsfrei volljährig, hat zusätzlich eine Ausweisprüfung zu erfolgen. Zweifel sind in Anlehnung an die Praxis bei der Kontrolle nach dem Jugendschutzgesetz, die seitens der in den einzelnen Bundesländern zuständigen Ministerien durch Erlasse bzw. Vollzugshinweise festgeschrieben wurde[2], dann gegeben, wenn durch das äußere Erscheinungsbild, das Verhalten oder Äußerungen der Eindruck entsteht, dass es sich um einen Minderjährigen handeln könnte. Erfolgt diese Ausweisprüfung per Webcam, gelten die vorgenannten Voraussetzungen auch hier. Es ist zudem sicherzustellen, dass der Ausweis von allen Seiten und vollständig in Augenschein genommen wird. Ist hiernach nicht zweifelsfrei festzustellen, dass der Nutzer volljährig ist, darf der Zugang nicht gewährt werden.

Bloße Personalausweiskennziffernprüfungen („Perso-Check-Verfahren“) oder die Vorlage einer Ausweiskopie sind dagegen nicht ausreichend. Auch eine beglaubigte Ausweiskopie reicht nicht aus, da hierbei nur die Übereinstimmung eines Dokumentes bestätigt wird, aber keine Identifizierung einer Person vorgenommen wird.

[2] Vgl. z.B. http://www.blja.bayern.de/textoffice/gesetze/juschg/anlagen.html

II. Konzepte der verlässlichen Altersprüfung für den wiederholten Nutzungsvorgang (Stichwort: „Generalschlüssel“)

Die verlässliche Altersprüfung für den wiederholten Nutzungsvorgang besteht aus zwei Schritten: einer einmaligen Identifizierung und einer Authentifizierung der identifizierten Person bei jedem Nutzungsvorgang. Nach der einmaligen Identifizierung wird dem als volljährig erkannten und somit berechtigten Nutzer eine Art „Generalschlüssel“ für alle folgenden Nutzungsvorgänge ausgehändigt. Damit wird ihm Zugriff zu einer beliebig großen Anzahl unterschiedlichster Angebote gewährt. Im Vergleich zum o.g. Einmalschlüssel oder im Vergleich zu einem Ladengeschäft mit Angeboten für Erwachsene (z. B. Videothek), in dem in der Regel nur eine limitierte Anzahl von Produkten erworben oder entliehen wird, sind entsprechend höhere Anforderungen zu stellen. Eine Altersüberprüfung über bloße Inaugenscheinnahme der Person genügt hier den Anforderungen nicht.

A. Identifizierung

Die Sicherstellung einer geschlossenen Benutzergruppe für Erwachsene ist nur mittels einer verlässlichen Altersprüfung bzw. Volljährigkeitsprüfung möglich. Voraussetzung für eine verlässliche Volljährigkeitsprüfung ist dabei die persönliche Identifizierung von natürlichen Personen inklusive Überprüfung ihres Alters. Die persönliche Identifizierung ist notwendig, damit Fälschungs- und Umgehungsrisiken möglichst vermieden werden.

Die Anforderungen der KJM sind folgendermaßen spezifiziert:

<u>Identifizierung und Überprüfung von Altersangaben:</u>

(1) Identifizierung im persönlichen Kontakt:

Die zumindest einmalige Identifizierung von Interessenten für eine geschlossene Benutzergruppe muss durch persönlichen Kontakt erfolgen. Unter **„persönlichem Kontakt“** ist verpflichtend eine Angesichts-Kontrolle

unter Anwesenden („face-to-face“-Kontrolle) mit Vergleich von amtlichen Ausweisdaten (Personalausweis, Reisepass) zu verstehen.

Dies ist z.B. der Fall bei Verfahren wie „Post-Ident“ oder vergleichbaren Verfahren.

Möglich ist es auch, unter bestimmten Bedingungen (s. unten) auf eine bereits erfolgte „face-to-face“-Kontrolle zurückzugreifen. Dies ist z.B. der Fall bei Identifizierungs-Verfahren mittels geprüfter Personen- und Alters- bzw. Geburtsdaten, die bereits bei Teilnahme an bestimmten Diensten bzw. Abschluss von bestimmten Verträgen (z.B. Mobilfunkverträgen, GwG-konforme Bankkonten-Eröffnung; Teilnahme am Kommunikationsdienst DE-Mail; Nutzung der eID-Funktion des neuen Personalausweises) unter Abgleich mit amtlichen Ausweisdaten erfasst wurden.

Bloße Personalausweiskennziffernprüfungen („Perso-Check-Verfahren“) oder die Vorlage bzw. Zusendung einer **Ausweiskopie** sind dagegen nicht ausreichend. Auch eine **beglaubigte Ausweiskopie reicht nicht aus**, da hierbei nur die Übereinstimmung eines Dokumentes bestätigt wird, aber keine Identifizierung einer Person vorgenommen wird.

Auch eine bloße **Identifizierung durch Webcams** bietet als initiale Altersprüfung für eine wiederholte Nutzungsmöglichkeit **keine** ausreichende Verlässlichkeit und genügt damit nicht den Anforderungen an eine verlässliche Identifizierung im Sinne der KJM-Eckwerte.

Soweit zusätzliche Sicherungsmaßnahmen ergriffen werden (vgl. diesbezüglich Ziffer III. des Rundschreibens 01/2104 GW der Bundesanstalt für Finanzdienstleistungsaufsicht[3]) kann dies jedoch den Anforderungen an eine verlässliche Identifizierung im Sinne der KJM-Eckwerte genügen.

[3] abrufbar unter http://www.bafin.de/dok/4992504

(2) Erfassung und Speicherung der für die Identifizierung notwendigen Daten:

Die für die Altersprüfung jeweils benötigten Personendaten der zu identifizierenden Person sollten in erforderlichem Maße unter Beachtung datenschutzrechtlicher Vorgaben erfasst und gespeichert werden (z.B. Geburtsdatum, Name, Adresse). Eine Erfassung nur des Alters der identifizierten Person ist nur dann ausreichend, wenn dieses im gleichen Schritt mit eindeutigen Authentifikationsmerkmalen verknüpft ist.

(3) Anforderungen an Erfassungsstellen:

Die Identifizierungsdaten können **an verschiedenen Stellen** erfasst werden (z.B. Postschalter, verschiedene Verkaufsstellen wie Ladengeschäfte von Mobilfunkanbietern, Lotto-Annahmestellen, ebenso Banken und Sparkassen etc.). Sicherzustellen ist eine **komplette Erfassung** der zur Altersprüfung relevanten **Personendaten** in einem Offline- oder Online-Formular und ihre **Weiterleitung an den AVS-Anbieter**. Alternativ zur Weiterleitung reicht auch die Übermittlung eines Referenzzeigers auf die erfassten Daten (speichernde Stelle, konkrete Fundstelle) an den AVS-Betreiber aus. Die Eignung einer Erfassungsstelle im Sinne des JMStV setzt ein **geschäftsmäßiges Anbieten durch zuverlässiges und in die Aufgabe hinreichend eingewiesenes Personal** voraus.

(4) abschließende Altersprüfung:

Der Zugang zur geschlossenen Benutzergruppe (Freischaltung der Benutzerdaten zur Authentifizierung) darf erst erfolgen, wenn der **AVS-Anbieter die Identifizierungsdaten bzw. einen Referenzzeiger auf diese erhalten und das Alter geprüft** hat. Nur mit den Daten der initialen Identifizierung kann der AVS-Anbieter bei jedem Betreten der geschlossenen Benutzergruppe prüfen, ob es sich um einen berechtigten erwachsenen Nutzer handelt (Authentifizierung).

Übermittlung von Zugangsschlüsseln an den Nutzer:

Werden Zugangsschlüssel (z.B. Freischalt-Codes, Hardwarekomponenten o.Ä.) nicht bereits während der Anmeldung persönlich an den Nutzer übergeben oder im Kontext der Anmeldung generiert, sondern ist eine Zustellung oder anderweitige Übermittlung im Nachhinein erforderlich, muss sichergestellt werden, dass die Zugangsschlüssel nur an die als volljährig identifizierte Person übermittelt werden.

Für den Fall, dass auf eine bereits erfolgte „face-to-face"-Kontrolle zurückgegriffen wird (s. oben) muss die Zustellung eines Zugangsschlüssels per Einschreiben eigenhändig oder durch eine ähnlich qualifizierte Variante erfolgen. Eine Variante ist dann ähnlich qualifiziert, wenn sie sicherstellt, dass nur die als volljährig identifizierte Person die Zugangsdaten erhält. Der Grund hierfür ist, dass eine anfangs nur behauptete Identität gegenüber einer tatsächlichen Identität verifiziert werden muss (s. oben). Eine anonyme Aushändigung oder Zustellung der Zugangsberechtigungen, z.B. mittels einfacher E-Mail oder über Kontoauszüge, ist somit nicht ausreichend. Vielmehr muss mit ausreichender Sicherheit davon ausgegangen werden, dass nur die zuvor als volljährig identifizierte Person Zugriff auf die Informationen erhält, die auf diesem Wege übermittelt werden (z.B. Zustellung mittels DE-Mail unter bestimmten Voraussetzungen,[4] durch rechtzeitigen und sicheren Abgleich der Kontenverbindung z.B. mit dem Namen des Kontoinhabers, Alter aller Verfügungsberechtigten etc.).

B. Authentifizierung

Die Authentifizierung dient der Sicherstellung, dass nur die jeweils identifizierte und altersgeprüfte Person Zugang zu geschlossenen Benutzergruppen erhält, und soll die Weitergabe von Zugangsberechtigungen an unautorisierte Dritte erschweren. Dabei muss Folgendes gewährleistet werden:

[4] vgl. dazu näher unten zur Stufe der Authentifizierung

Zugangsgewährung gegenüber Nutzern:

- Vornahme einer Authentifizierung eingangs jeden Nutzungsvorgangs („Sitzung“).
- **Sicherung von Inhalten im Sinne des § 4 Abs. 2 JMStV durch ein spezielles, individuell zugeteiltes Passwort** (nicht notwendig bei biometrischen Verfahren, da dabei die berechtigte Person zweifelsfrei identifiziert wird)

Verhinderung der Weitergabe/ Multiplikation:

Es sind ausreichende Schutzmaßnahmen zur Erschwerung der Multiplikation und der Nutzung von Zugangsberechtigungen durch unautorisierte Dritte zu ergreifen. Der Weitergabeschutz kann dabei entweder durch technische Maßnahmen zur Erschwerung der Multiplikation (s. Lösungsvariante 1: Hardware-Lösung/ Unique-Identifier-Lösung) oder durch persönliche Risiken in der Sphäre des Benutzers (s. Lösungsvariante 2: Risiko-Lösung) realisiert werden.

Lösungsvariante 1:
Mögliche technische Maßnahmen zur Erschwerung einer Multiplikation von Zugangsberechtigungen → HARDWARE- oder UNIQUE-IDENTIFIER-LÖSUNG:

- **Prüfung biometrischer Daten:** Zugang zur geschlossenen Benutzergruppe können nur im Vorfeld identifizierte Nutzer bekommen, die sich dann über biometrische Daten (z. B. Fingerprint, Iris-Erkennung) authentifizieren können. Zugangsberechtigungen können nicht multipliziert oder von Dritten genutzt werden, sofern bei der Erfassung der biometrischen Daten und der Authentifizierung hinreichend sichere Verifikationskomponenten benutzt werden.

- **Aktive Hardwarekomponente:** Aktive Hardware (z.B. ID-Chip, SIM-Karte) hat die Fähigkeit, dass auf dem Chip Rechenoperationen durchgeführt werden können. Sie kann nur mit großem Aufwand

reproduziert werden. Die Zugangsberechtigung (Hardware + Passwort) kann deshalb nur sequentiell jeweils an eine einzelne Person weitergegeben werden.

- **Passive Hardwarekomponente:** Passive Hardware-Lösungen (z.B. passive Chip-Karten, auch DVD, CD-ROM) haben im Gegensatz zu aktiver Hardware nur die Fähigkeit zu speichern und sind bauartbedingt nicht mit eigener CPU ausgestattet. Unter bestimmten Umständen können diese Komponenten jedoch ausgelesen und vervielfältigt bzw. die Kommunikation des Endgerätes mit der Hardware kann emuliert werden. Daher dürfen diese Komponenten nicht trivial kopierbar sein und – soweit sie auslesbar sind – darf eine nicht bestimmungsgemäße Nutzung des Ausgelesenen nicht möglich sein.

- **One-Time-PIN-Verfahren (z.B. mit Token-Generator oder One-Time-PIN per SMS an registrierte SIM-Karte):** PIN-TAN-Listen gewährleisten keinen ausreichenden Multiplikationsschutz, da hier prinzipiell vielfältige Zugänge verfügbar sind. Ausreichend sind dagegen One-Time-PIN-Verfahren, bei denen eine kopiergeschützte Hardware zu Generierung oder Empfang von nur einmalig nutzbaren Zugangsberechtigungen verwendet wird.

- **Identifizierung des Endgerätes:** Hier wird der Rechner selbst bzw. das jeweilige Ausgabegerät zum Schutz vor Multiplikation und Weitergabe von Zugangsberechtigungen eingesetzt (z.B. Abfrage der Prozessor-ID). Durch eine entsprechende Kombination von Zugangssoftware und Hardware des Endgerätes kann mit ausreichender Sicherheit gewährleistet werden, dass eine Zugangsberechtigung nur auf einem einzigen Endgerät genutzt werden kann.

Lösungsvariante 2:
Subjektive Erschwerung von unautorisierter Nutzung von Zugangsberechtigungen in der Sphäre des Benutzers (Reduzierung des Risikos der Weitergabe) → RISIKOLÖSUNG:

Das Risiko, dass der berechtigte Nutzer seine Zugangsberechtigungen selbst an unautorisierte Dritte weiter gibt, kann dadurch reduziert werden, dass ihm dabei erhebliche materielle oder immaterielle Nachteile entstehen können. Hierauf muss der Nutzer im Rahmen des Anmeldevorgangs deutlich hingewiesen werden. Ob ein Weitergaberisiko ausreicht, ist dabei an der vermuteten „Spürbarkeit" der Nachteile im Einzelfall festzumachen. Nicht ausreichend ist es, wenn sich diese lediglich in rein virtuellen Lebensbereichen niederschlagen.

Erhebliche Nachteile im o.g. Sinne sind z.B. dann zu vermuten, wenn bei der Weitergabe der Daten das dauerhafte Risiko besteht, dass hohe Kosten entstehen und / oder wichtige Geheimnisse preisgegeben werden:

- **Kosten-Risiko:** Ein hohes finanzielles Risiko ist z.B. dann gegeben, wenn bei der Nutzung der Zugangsberechtigung das Girokonto oder die Kreditkarte des berechtigten Nutzers in relevanter Höhe und dauerhaft belastet werden kann. Prepaid-Verfahren ohne weitergehendes finanzielles Risiko reichen hierfür nicht aus.

- **Geheimnis-Risiko:** Ein hohes Risiko in Bezug auf die Preisgabe von Geheimnissen ist z.B. dann gegeben, wenn ein unberechtigter Dritter bei der Nutzung der Zugangsberechtigung Einblick in relevante (höchst-) persönliche Lebensbereiche des Nutzers bekommen und diese Informationen ggf. auch eigenmächtig verändern kann wie z.B. Gesundheitsdaten, Zahlungsverkehrsinformationen etc.

Idealtypischer Weise sind derartige Risiken in Kombination gegeben. Ist dies nicht der Fall, ist hinsichtlich des Kostenrisikos zu fordern, dass der Zugang unverzüglich storniert wird, wenn das Konto des Nutzers nicht gedeckt ist.