

Entscheidung 03656 - I

Zusammenfassung:

Die Beschwerdegegnerin ist Mitglied der FSM und unterhält unter diversen Domains kostenpflichtige Bereiche, in denen teilweise entwicklungsbeeinträchtigende sowie vor allem „in sonstiger Weise“ pornografische Inhalte i.S.d. § 4 Abs. 2 Satz 1 Ziffer 1 JMStV abrufbar sind. Deren Verbreitung in Telemedien ist nach § 4 Abs. 2 S. 2 JMStV nur zulässig, wenn von Seiten des Anbieters sichergestellt ist, dass sie nur Erwachsenen innerhalb einer sog. „geschlossenen Benutzergruppe“ zugänglich gemacht werden.

Der Beschwerdegegnerin wurde vorgeworfen, nicht ausreichend sicherzustellen, dass Minderjährige auf ihre Angebote nicht zugreifen können.

Die Beschwerdegegnerin reduzierte nach Abhilfeaufforderung der Beschwerdestelle der FSM ihre bis dahin große Anzahl vorhandener (und oftmals nicht ausreichender) Altersverifikationsverfahren. Des Weiteren hat sie die Verfahren umfassend verbessert. Bei den verbliebenen 5 Altersverifikationsverfahren gelangte der Beschwerdeausschuss zu der Auffassung, dass 4 von ihnen den gesetzlichen Vorgaben genügen. Bezüglich des unzureichenden Verfahrens (Webcam-Check) wurde die Beschwerdegegnerin aufgefordert, diese Version als Identifikationsmaßnahme für ihre Angebote nicht mehr einzusetzen, bzw. die bisherige Version insoweit zu verbessern, dass sie den Anforderungen des § 4 Abs. 2 S. 2 JMStV entspricht.

(gesamte Entscheidung siehe unten)

Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.

In der Sache

AX

Straße

Ort

FSM-Beschwerde Nr. 03656

ENTSCHEIDUNG

Die Beschwerdestelle der Freiwilligen Selbstkontrolle Multimedia (FSM) e.V. hat vorbezeichnete Beschwerde an den Beschwerdeausschuss weitergeleitet. Der Beschwerdeausschuss hat die Beschwerde der Beschwerdeführerin in der Besetzung XY, XZ, XA in seiner Sitzung vom 22.06.2006 beraten und entschieden:

- I. Der Beschwerdegegnerin wird ein Hinweis mit Abhilfeaufforderung erteilt und aufgegeben, Wiederholungen dieser Art zu unterlassen.
- II. Zur Abhilfe wird eine Frist von 14 Tagen ab Bekanntgabe dieser Entscheidung eingeräumt.
- III. Im Übrigen wird das Verfahren auf Grund Selbstabhilfe durch die Beschwerdegegnerin eingestellt.

Begründung

I. Sachverhalt

1. Die Beschwerdegegnerin ist Mitglied der FSM und unterhält unter der URL <http://www...de> sowie unter einer Vielzahl von weiteren einzelnen Domains, Angeboten und Verlinkungen (z.B. <http://www...de>, <http://www...de>, <http://www...de> und andere) kostenpflichtige Bereiche, in denen teilweise entwicklungsbeeinträchtigende sowie vor allem „in sonstiger Weise“ pornografische Inhalte i.S.d. § 4 Abs. 2 Satz 1 Ziffer 1 JMStV abrufbar sind. Deren Verbreitung ist in Telemedien nur zulässig, wenn von Seiten des Anbieters sichergestellt ist, dass sie nur Erwachsenen

innerhalb einer sog. „geschlossenen Benutzergruppe“ zugänglich gemacht werden. Die Nutzung dieser Bereiche ist kostenpflichtig und teilweise im Abo-System mit monatlicher Zahlungsweise (z.B. bei <http://www.de>) organisiert. Der Nutzer muss dort bei der Erstanmeldung nach Eingabe eines selbstgewählten Usernamens (mind. 6-stellig) und seiner gültigen E-Mail-Adresse sowie weiterer persönlicher Daten zwischen der Bezahlung per Lastschrift oder Kreditkarte wählen, wobei ausschließlich eine auf den Namen des Nutzers lautende persönliche inländische Girokontenverbindung oder eine solche Kreditkarte akzeptiert werden.

Die Beschwerdegegnerin nutzt für die Zahlungsabwicklung das Zahlungssystem „ABCDEFGH“ (teilweise auch noch das ähnlich funktionierende System „HIJKLMN“) mit integrierter Bezahlungsfunktion, so dass der Kunde nach erfolgter Anmeldung und Erstbelastung des Kontos / der Kreditkarte, anschließendem Alterscheck (vgl. hierzu die Ausführungen unten) und Freischaltung mit seinem Passwort auch auf teils erhebliche Mehrkosten verursachende Angebote der Beschwerdegegnerin sowie auf zusätzliche kostenpflichtige Angebote von an ABCDEFGH angeschlossene Drittanbieter zugreifen kann, deren Abrechnung und Belastung ebenfalls direkt auf die bei der Anmeldung angegebene deutsche Bankverbindung oder Kreditkarte erfolgt.

Schon mit der Erstanmeldung wird dem Nutzer vor Freischaltung beim Abo-System mit monatlicher Zahlungsweise (z.B. bei <http://www.de>) der erste Monatsbeitrag berechnet. Der Nutzer erhält nach erfolgter Belastung der von ihm angegebenen Girokontenverbindung oder Kreditkarte eine Zahlungsbestätigung an die von ihm eingegebene E-Mail-Adresse mit Bekanntgabe eines sog. Master-Passwortes. Ein Zugriff auf die Angebote im Sinne des § 4 Abs. 2 S.1 ist jedoch - nicht nur im Abo-System - erst nach erfolgter zusätzlicher Altersverifikation (dazu näher unten) und anschließender Freischaltung möglich. In der Zwischenzeit erhält der User nur einen Zugriff auf als „Softangebote“ deklarierte Angebote.

Sollte dieser erste Bezahlvorgang nicht ordnungsgemäß abgewickelt werden können (z.B. aufgrund Nicht-Existenz der angegebenen Kontenverbindung / Kreditkartennummer oder Mitteilung der abwickelnden Bank bei Nicht-Übereinstimmung des vom Nutzer angegebenen Namens mit dem tatsächlichen Konteninhaber), wird das weitere Anmeldeverfahren nicht fortgesetzt bzw. abgebrochen. Der Kunde wird dann von Seiten der Beschwerdegegnerin nicht freigeschaltet bzw. der Versand einer Freischalt-PIN durch die Beschwerdegegnerin unterbleibt. Eine Freischaltung bzw. der Versand der Freischalt-PIN unterbleiben bei nicht

korrekter Zahlungsabwicklung auch für den Fall, dass ein zwischenzeitlich erfolgter Alterscheck die Volljährigkeit des angemeldeten Kunden ergeben hat.

2. Die Beschwerdeführerin wirft der Beschwerdegegnerin einen Verstoß gegen § 4 Abs. 2 S. 2 JMStV vor. Die Beschwerdeführerin macht geltend, dass bei dem Angebot der Beschwerdegegnerin nicht ausreichend sichergestellt sei, dass Minderjährige nicht zugreifen können.

Der von der Beschwerdegegnerin im Anschluss an den Anmeldevorgang und nach erfolgtem Zahlungsvorgang (s.o.) geforderte Altersnachweis und die Freischaltung für den Zugang waren zum Zeitpunkt des Eingangs der Beschwerde bei der FSM aufgrund der Online-Kurzbeschreibung der Beschwerdegegnerin wie folgt möglich:

- a) Ausweiskopie per Post/Fax/E-Mail - anschließend sofortige Freischaltung
- b) Eingabe von Personalausweis-Nummer und Sozialversicherungsnummer - anschließend sofortige Freischaltung (nur bei HIJKLMN)
- c) Foto des Anmeldenden mit Username auf einem Zettel - sofortige Freischaltung nach Kontrolle des Fotos per E-Mail durch Support-Mitarbeiter der Beschwerdegegnerin
- d) Foto des Anmeldenden mit Username auf einem Zettel - sofortige Freischaltung nach Kontrolle des Fotos per MMS durch Support-Mitarbeiter der Beschwerdegegnerin
- e) Altersnachweis per Webcam - sofortige Freischaltung nach Kontrolle durch Support-Mitarbeiter (Webcam-Check)
- f) Eingabe einer deutschen Giro-Kontenverbindung - Erhalt einer Freischalt-PIN durch Überweisungsvermerk im Kontoauszug (Konto-Pin)
- g) Eingabe bestimmter persönlicher Daten - Erhalt einer Freischalt-PIN mittels „persönlichem“ neutral aussehenden Brief - Freischaltung nach Brief-Erhalt (Brief-Pin)
- h) Alterscheck mittels Geldkarte oder Girokonto-Karte mit Geldkartenchip (jeweils Karte mit Altersmerkmal) über Geldkarten-Lesegerät am PC des Nutzers - Freischaltung sofort
- i) Alterscheck mittels Post-Ident-Verfahren - Freischaltung nach Eingang des Nachweises bei der Beschwerdegegnerin.

3. Nach Eingang der Beschwerde der Beschwerdeführerin bei der Beschwerdestelle der FSM wurde der Beschwerdegegnerin Gelegenheit zur Stellungnahme und Abhilfe gegeben. Die Beschwerdegegnerin beschränkte daraufhin die Möglichkeiten der Anmeldung, Altersverifizierung und Freischaltung auf folgende Varianten:

1. **Post Ident:** Anmeldung unter Angabe von u.a. Vor- und Nachname, genauer Anschrift und Geburtsdatum, sowie persönlicher inländischer Kontenverbindung bzw.

persönlicher Kreditkartennummer mit sofortiger Kontenbelastung; anschließend Alterscheck mittels Post-Ident-Verfahren - Freischaltung des Bereichs der geschlossenen Benutzergruppe nach Eingang des Altersnachweises bei der Beschwerdegegnerin.

2. **Brief-PIN:** Anmeldung unter Angabe von u.a. Vor- und Nachname, genauer Anschrift und Geburtsdatum sowie persönlicher inländischer Kontenverbindung bzw. persönlicher Kreditkartennummer mit sofortiger Kontenbelastung; anschließend Altersverifizierung durch erneute Eingabe der persönlichen Daten; sofortiger („on-the-fly“) Schufa-Abgleich der eingegebenen Namens- und Adresdaten sowie des exakten Geburtsdatums; nach Schufa-Bestätigung Erhalt einer Freisicht-PIN mittels Einschreiben „eigenhändig“ - Freischaltung nach Brief-Erhalt und Eingabe der 7-stelligen PIN durch den Nutzer (max. 5 Fehlversuche zulässig).

3. Konto-Pin

4. Geldkarten-Check

5. Webcam-Check

4. Mit schriftlicher Stellungnahme vom xx.yx.2006 sowie mündlicher Erläuterung vom xx.xx.2006 wurden dem Beschwerdeausschuss die Einzelheiten der nunmehr verbliebenen Anmeldevarianten erläutert. Bzgl. der Einzelheiten vgl. die schriftliche Stellungnahme der Beschwerdegegnerin vom xx.xy.2006 (Version x.x) sowie die anschließenden Entscheidungsgründe.

II. Entscheidungsgründe

1. Grundlagen der Entscheidung und Prüfumfang

Grundlage der Entscheidung waren die Bestimmungen des Jugendmedienschutz-Staatsvertrags (JMStV) i.d.F. vom 01.04.2003, die einschlägigen Vereinsdokumente der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter e.V. (FSM), die gemeinsamen Richtlinien der Landesmedienanstalten zur Gewährleistung des Schutzes der Menschenwürde und des Jugendschutzes (Jugendschutzrichtlinien - JuSchRiL) vom 8./9.

März 2005 sowie die entsprechenden Veröffentlichungen der Kommission für Jugendmedienschutz (KJM).

Da die Beschwerdegegnerin nach erster Abhilfeaufforderung durch die Beschwerdestelle der FSM die Anmeldung zu ihren Angeboten sowie insbesondere die Alterskontrolle auf nunmehr nur noch fünf tatsächlich eingesetzte Varianten beschränkt hat, bildeten diese verbliebenen Varianten den Gegenstand der Beurteilung des hier entscheidenden Beschwerdeausschuss.

3. Nur teilweise ausreichende Altersverifikation (§ 4 Abs. 2 S. 2 JMStV) nach Abhilfe

Die von der Beschwerdegegnerin angebotenen Inhalte verstoßen teilweise gegen § 4 Abs. 2 S. 1 Ziff. 1 und Ziff. 3 JMStV (Jugendmedienschutz-Staatsvertrag): Die bereitgestellten Inhalte sind teilweise pornografisch und offensichtlich geeignet, die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit schwer zu gefährden. In Telemedien sind solche Angebote nur zulässig, wenn von Seiten des Anbieters sichergestellt ist, dass die angebotenen Inhalte nur Erwachsenen zugänglich gemacht werden (§ 4 Abs 2 S. 2 JMStV – „geschlossene Benutzergruppe“).

Von Seiten des Anbieters, also der Beschwerdegegnerin, ist nach erster Abhilfe jedenfalls für die Variante des **Webcam-Checks** derzeit aber noch **nicht** ausreichend sichergestellt, dass die angebotenen Inhalte nur Erwachsenen zugänglich gemacht werden (§ 4 Abs 2 S. 2 JMStV – „geschlossene Benutzergruppe“).

Wie eine geschlossene Benutzergruppe erreicht werden kann, definiert das Gesetz nicht und ist für den heutigen Stand der Technik nicht abschließend geklärt:

Nach der Auffassung des Beschwerdeausschusses ist - unter Berücksichtigung der Vorgaben der Jugendschutzrichtlinien sowie in Anlehnung an die Entscheidung des Gemeinsamen Ausschusses der FSM vom 16.07.2004 zur Frage der Altersverifikationssysteme (AVS) - zum sicheren Altersnachweis im Telemedienbereich nach derzeitigem technischen Stand ein zweistufiges Verfahren erforderlich:

1. Identifizierung des Nutzers mit sicherer Volljährigkeitsprüfung (z.B. durch persönliche Identifikation anhand eines vorzulegenden gültigen Personaldokuments oder ein gegenüber der persönlichen Identifikation gleichwertiger Altersnachweis durch eine hinreichend zuverlässige Person oder Stelle, wobei der Nachweis auch durch entsprechend sichere technische Verfahren gewährleistet sein kann)

2. Authentifizierung des Nutzers bei jedem Nutzungsvorgang, so dass jedenfalls eine massenhafte Weitergabe und Verbreitung von Zugangsdaten verhindert wird.

a) Erste Stufe: Identifizierung

Im Zuge der „Identifizierung“ wird im Rahmen der Anmeldung und Altersverifikation durch vier von der Beschwerdegegnerin nunmehr eingesetzte Verfahren - mit Ausnahme des Webcam-Checks - hinreichend sichergestellt, dass der Nutzer das 18. Lebensjahr vollendet hat.

aa) Erste Variante: Altersverifizierung mittels Post-Ident-Verfahren ausreichend

Das von der Beschwerdegegnerin als erste Variante eingesetzte Post-Ident-Verfahren ist zum Nachweis der Volljährigkeit auf der Stufe der Identifizierung zweifelsohne geeignet: Der Nutzer wird in einer Filiale der Deutschen Post AG anhand seines gültigen Personalausweises oder Reisepasses eindeutig identifiziert. Ein Angestellter der Deutschen Post AG überprüft persönlich die Identität des Nutzers und trägt dessen Personaldaten in ein entsprechendes Formular ein (u.a. Vorname, Nachname, Straße, Hausnr., Ort, exaktes

Geburtsdatum, Ausstelldaten des Ausweises). Außerdem wird in dem Formular eine dem Nutzer zuvor zugeteilte Referenznummer der Beschwerdegegnerin vermerkt. Das ausgefüllte, vom Angestellten der Deutschen Post AG gegengezeichnete und abgestempelte Formular, dessen Blanko-Vordruck nicht im öffentlichen Publikumsverkehr erhältlich ist, wird von der Deutschen Post AG direkt an die Beschwerdegegnerin gesandt, die den Nutzer anhand der Referenznummer eindeutig identifizieren, seine Volljährigkeit nochmals nachprüfen (Geburtsdaten von Minderjährigen werden vom System der Beschwerdegegnerin von vornherein technisch nicht akzeptiert) und dann für die geschlossene Benutzergruppe freischalten kann.

Da das Post-Ident-Formular keinerlei Zugangsdaten (Username oder Passworte) enthält, kann auch eine missbräuchliche Nutzung z.B. durch hiervon Kenntnis erhaltende Minderjährige oder sonstige Dritte mit hinreichender Sicherheit ausgeschlossen werden.

bb) Zweite Variante: Altersverifizierung über „Brief-PIN“ nach Schufa-Datenabgleich und Einschreiben „eigenhändig“ ausreichend

Auch das von der Beschwerdegegnerin als zweite Variante eingesetzte Brief-PIN-Verfahren ist in seiner konkreten Ausgestaltung zum Nachweis der Volljährigkeit auf der Stufe der Identifizierung als hinreichend anzusehen: Das Zusammenspiel und Ineinandergreifen mehrerer Kontrollroutinen führt dazu, dass auch hier ein „Sicherstellen“ iSd § 4 Abs. 2 S. 2 JMStV anzunehmen ist.

ICRA / JusProg-Label

Festzuhalten ist insoweit aber, dass die Möglichkeit eines von Seiten der Erziehungsberechtigten eingesetzten Filters (z.B. IRCA / JusProg), welche einen Zugriff auf gekennzeichnete (gelabelte) Seiten der Beschwerdegegnerin mittels eines nutzerautonomen Jugendschutzprogramms verhindern können, nichts ändert an der dem Wortlaut des § 4 Abs. 2 S. 2 JMStV entnehmbaren eindeutigen gesetzlichen Verpflichtung des Anbieters, seinerseits (d.h. „von Seiten des Anbieters“) zuverlässig sicherzustellen, dass bestimmte Angebote in Telemedien nur Erwachsenen zugänglich gemacht werden.

Abgleich der Postanschrift

Der von der Beschwerdegegnerin zunächst durchgeführte Online-Abgleich der eingegebenen Adressdaten (bei dem lediglich geprüft wird, ob die eingegebene Postleitzahl tatsächlich mit der angegebenen Straße übereinstimmt) mit der Straßen-Datenbank der Deutschen Post AG ist als Nachweis für eine Volljährigkeit für sich genommen allerdings noch nicht geeignet, da er keinerlei personenbezogene Kontrolle und insbesondere keinen Altersabgleich durchführt.

Angabe einer existierenden E-Mail-Verbindung

Auch die Angabe einer gültigen E-Mail-Adresse (an welche die Begrüßungsmail des Bezahlsystems ABCDEFG mit dem Usernamen sowie dem Master-Passwort geschickt wird) kann für eine Altersverifikation noch keine Rolle spielen, da eine solche E-Mail-Adresse ohne weiteres auch von einem Minderjährigen unterhalten werden kann. Bedeutsam ist jedoch, dass ein Zugriff auf die Inhalte gem. § 4 Abs. 2 JMStV nicht schon nach Erhalt der Begrüßungsmail mit dem dort angegebenen Usernamen sowie dem Passwort möglich ist, sondern erst nach zusätzlichem Schufadaten- sowie ggf. Bankdatenabgleich und PIN-Versand in einem Einschreiben „eigenhändig“ (dazu sogleich).

Schufa-Identitätsprüfung

Entscheidend für eine Verifizierung der Volljährigkeit des Anmeldenden ist der Online-Abgleich der eingegebenen Personaldaten incl. des exakten bei der Erstanmeldung eingegebenen Geburtsdatums des Users mit dem Datenbestand der SCHUFA Holding AG (im Folgenden: Schufa).

Hierfür verwendet die Beschwerdegegnerin nicht ausschließlich Datensätze des von der KJM bereits begutachteten und mit Entscheidung vom September 2005 für ausreichend erachteten Moduls „Identitäts-Check mit Q-Bit“, bei dem nachweisbar ein durch eine Face-to-Face-Kontrolle verifiziertes Datenmaterial zur Verfügung steht und welches als solches bei der konkreten Anfrage auch gekennzeichnet wird. Zum Abgleich werden dort nur Daten von Kreditinstituten genutzt, die die Volljährigkeitsprüfung gemäß den Vorgaben des Geldwäsche-Gesetzes (GWG) durchführen. Soweit der Abgleich der durch die Beschwerdegegnerin an die Schufa gemeldeten Anmeldedaten des Nutzers incl. exaktem Geburtsdatum in der Auskunft der Schufa resultiert, dass es sich hierbei um einen Q-Bit-Datensatz handelt, kann jedenfalls von einer hinreichend sicheren Identifizierung auf der

ersten Stufe der Altersverifikation ausgegangen werden (zum weiteren von der KJM verlangten Erfordernis einer Auslieferung der Zugangsdaten eigenhändig per Einschreiben: vgl. unten)

Die Beschwerdegegnerin hat sich darüber hinaus für eine Einbeziehung sämtlicher (also nicht nur der Q-Bit) Schufa-Datensätze entschieden, so dass auch die restlichen Datensätze - derzeit weniger als 15% aller Schufa-Datensätze mit weiter abnehmender Tendenz - zum Abgleich und Identitäts- / Volljährigkeitsnachweis herangezogen werden. Durch ein Zusammenspiel mit den übrigen von der Beschwerdegegnerin eingesetzten, im Folgenden näher beschriebenen und vom hiesigen Beschwerdeausschuss bewerteten Kontrollmechanismen kann jedoch auch hier nach derzeitigem Stand der Technik von einer hinreichend sicheren Identifizierung auf der ersten Stufe der Altersverifikation ausgegangen werden. Das verbleibende Restrisiko, dass eine bei der Schufa als erwachsen registrierte Person tatsächlich noch minderjährig ist, ist im Ergebnis vernachlässigbar gering. Namentlich das Zusammenspiel und Ineinandergreifen von Schufa-Auskunft, zwingender persönlicher Konten-/Kreditkarteninhaberschaft des Nutzers mit Abbuchung vor Freischaltung sowie Zusendung einer Brief-PIN mittels eigenhändigem Einschreiben kann eine solche Bewertung für das Altersverifikationsverfahren der Beschwerdegegnerin rechtfertigen:

- Die Beschwerdegegnerin lässt kumulativ folgende vom Nutzer eingegebene Daten über eine eigene Online-Schnittstelle mit dem Datenbestand der Schufa abgleichen:

Vorname, Nachname, Straße, Hausnummer, Postleitzahl, Ort, exaktes Geburtsdatum. Nur wenn der Nutzer aufgrund aller dieser Angaben in der Datenbank der Schufa eindeutig identifiziert und darüber hinaus seine Volljährigkeit bestätigt werden kann, wird das Altersverifikationsverfahren weiter fortgeführt. Sollte in der Schufa-Datenbank ein Datensatz auf die entsprechende Person (Name und Adresse) existieren, welcher gar kein oder nicht das exakte zum Abgleich angebotene Geburtsdatum enthält, wird das Verfahren automatisiert abgebrochen. Gleiches passiert, soweit das Geburtsdatum eines offensichtlich noch Minderjährigen abgeglichen werden soll.

- Sämtliche in der geschlossenen Benutzergruppe verfügbaren Inhalte sind kostenpflichtig und (insbes. bei den Angeboten über [http://www.de](http://www...de)) für einen monatlichen Abo-Beitrag abrufbar. Sofern die Abbuchung der Gebühren über ein

inländisches Girokonto mittels Lastschrift oder über eine Kreditkarte erfolgt, welche zwingend auf den Namen des anmeldenden Nutzers lauten müssen, ist dieses Verfahren hinreichend sicher für die Stufe der Identifizierung. Der anmeldende Kunde muss zwingend über ein Girokonto verfügen. Sollte sich bei der Anmeldung und der dort erfolgenden ersten Abbuchung eine Nicht-Übereinstimmung von Kontoinhaber oder Kreditkarteninhaber mit dem angegebenen Namen des Nutzers ergeben, erhält die Beschwerdegegnerin unverzüglich eine Mitteilung ihrer Bank über die Diskrepanz und bricht das weitere Altersverifikations- und Freischaltverfahren umgehend ab. Die Mitteilung und der Abbruch des Freischaltverfahrens erfolgen in der Regel vor Versand der Freischalt-PIN, jedenfalls aber - wegen der üblichen Postlaufzeiten - vor einem Eintreffen der Brief-PIN beim Besteller.

Sollte hingegen keine Mitteilung der Bank erfolgt sein, kann davon ausgegangen werden, dass auf den Anmelder - dessen übrige Daten zwingend ja schon mit dem Schufa-Bestand abgeglichen und bestätigt wurden - auch tatsächlich die angegebene (Giro-) Kontenverbindung existiert. Da fast alle deutschen Kreditinstitute in der Bundesrepublik Deutschland an die Schufa angeschlossen sind, kann mit an Sicherheit grenzender Wahrscheinlichkeit in diesem Fall auch davon ausgegangen werden, dass seine in der Schufa-Datenbank enthaltenen Daten - soweit sie bei der Schufa nicht schon ausdrücklich als Q-Bit-Datensatz vermerkt sind - dennoch im Rahmen der Datenerfassung nach dem Geldwäschegesetz erhoben worden sind und damit durch Vorlage eines gültigen amtlichen Ausweisdokuments durch die kontoführende Bank verifiziert wurden. Allenfalls bei Kontenverbindungen und damit bei Datensätzen, die noch vor Inkrafttreten des Geldwäschegesetzes im Oktober 1993 angelegt und seitdem nicht wieder überprüft und aktualisiert wurden, könnte ein Abgleich mit einem Ausweisdokument aufgrund bis dahin fehlender gesetzlicher Verpflichtung unterblieben sein. Bei solchen Daten kann jedoch davon ausgegangen werden, dass ein zum damaligen Zeitpunkt evtl. noch minderjähriger Konteninhaber

mittlerweile sicherlich volljährig geworden ist: Ausgehend vom Zeitpunkt hiesiger Beschwerdeentscheidung müsste rein rechnerisch ein noch zum heutigen Zeitpunkt Minderjähriger bei der damaligen - ohne Ausweiskontrolle erfolgten - Eröffnung seines Girokontos oder Ausstellung seiner auf ihn lautenden Kreditkarte noch nicht einmal sechs Jahre alt gewesen sein - ein schon von Seiten der Banken unter praktischen und rechtlichen (Geschäftsunfähigkeit) Gesichtspunkten nahezu undenkbares Ergebnis.

Für den Sonderfall, dass ein Minderjähriger (in der Regel mit Zustimmung seiner gesetzlichen Vertreter) tatsächlich Inhaber eines Girokontos ist, würde aber schon die Abfrage bei der Schufa kein positives Ergebnis bringen, da Geburtsdaten von Minderjährigen bei der Schufa regelmäßig nicht gespeichert werden und daher keinen für den Altersabgleich validen Datensatz liefern könnten. Falls das Geburtsdatum eines Minderjährigen dennoch in der Schufa-Auskunft enthalten sein sollte, wird spätestens im Zeitpunkt des Datenabgleichs die so als minderjährig identifizierte Person für das weitere Verfahren automatisch gesperrt.

Theoretisch denkbar wäre allenfalls, dass ein Minderjähriger versucht, eine Scheinidentität bei der Schufa durch Bestellvorgänge z.B. bei Versandhäusern gezielt aufzubauen, um sich Zugang zu Erwachseneninhalten zu verschaffen. Diese theoretische Möglichkeit der Umgehung wird aber schon aus eigenem Interesse an einer möglichst hohen Datenqualität der Schufa durch spezielle „Fraud Prevention Systeme“ der beteiligten Versandhäuser weitestgehend kontrolliert und verhindert. Darüber hinaus werden von Partnerunternehmen der Schufa neu eingelieferte (und ggf. vom Nutzer gefälschte) Datensätze, die nicht das Q-Bit-Merkmal tragen, grundsätzlich innerhalb von 10 Tagen wieder gelöscht und stehen danach für einen weiteren Abgleich sowieso nicht mehr zur Verfügung.

Ein dennoch verbleibendes Restrisiko bedeutet zwar, dass eine 100%ige Sicherheit nicht erreicht werden kann. Dies ist jedoch auch durch § 4 Abs. 2 JMStV nicht gefordert, da dieser keine höheren Anforderungen als in der Offline-Welt (z.B. in einem Ladengeschäft) aufstellen möchte und da dieser ansonsten einem verfassungsrechtlich nicht erwünschten Totalverbot gleichkäme. Ein solches Ergebnis wäre vom Gesetz nicht gewollt, da es eine „geschlossene Benutzergruppe“ ausdrücklich zulässt

- Durch die anschließende Zusendung der Brief-PIN per Einschreiben „eigenhändig“ an den mittels Schufa- und ggf. Bankauskunft als volljährig identifizierten Nutzer ist zudem gewährleistet, dass keine andere (minderjährige) Person die Brief-PIN durch Vorspielung einer anderen Identität (z.B. Angabe der Daten eines Elternteils inkl. dessen Kontenverbindung, welche einem Minderjährigen bekannt sein könnten) erreichen kann. Die Brief-PIN würde an die volljährige Person geschickt werden und nicht an den Minderjährigen. Sollte der Abgleich der Schufa-Daten nicht bereits auf

einem Datensatz beruhen, der auf eine Face-to-Face-Kontrolle zurückzuführen ist, so wird eine solche spätestens in dem Zeitpunkt gewährleistet, in dem der Postzusteller die Freischalt-PIN mittels Einschreiben „eigenhändig“ dem - zuvor vom System als

volljährig identifizierten - Nutzer zustellt. Denn spätestens an dieser Stelle erfolgt durch den zustellenden Postbediensteten eine (bei Q-Bit-Daten dann sogar doppelte) Face-to-Face Kontrolle anhand der Vorlage eines gültigen Ausweisdokuments, um die Empfangsberechtigung nachzuweisen. Zwar erfolgt an der Haustür keine direkte Altersüberprüfung mehr, wohl aber eine sichere Identifikation der Person, deren Alter zuvor durch den Datensatz der Schufa eindeutig inklusive der exakten Geburtsdaten als volljährig identifiziert wurde.

Da dieser Verifikationsschritt in jedem Fall durchlaufen werden muss, ist nach Auffassung des Beschwerdeausschusses eine hinreichend sichere Altersüberprüfung gegeben. Die Identifikationsstufe erfüllt sowohl die Anforderungen der FSM als auch der Landesmedienanstalten nach Ziff. 5.1 der Jugendschutzrichtlinie, da sie ein vergleichbares Schutzniveau erreicht.

Zahlungsabwicklungsmodalitäten

Sollte die Schufa-Auskunft positiv ausgefallen sein, bieten auch die Zahlungsmodalitäten zusätzlich Gewähr für die Volljährigkeit der Nutzer. Sämtliche in der geschlossenen Benutzergruppe verfügbaren Inhalte sind kostenpflichtig und für einen monatlichen Abo-Beitrag abrufbar. Die Abbuchung der Gebühren erfolgt (insbes. bei den Angeboten über [http://www.de](http://www...de)) über ein inländisches Girokonto oder über eine Kreditkarte, welche zwingend auf den Namen des anmeldenden Nutzers lauten müssen. Die erste Abbuchung erfolgt unmittelbar nach dem ersten Anmeldevorgang und regelmäßig noch vor Versand der Freischalt-PIN mittels eigenhändigem Einschreiben. Sollte sich eine Nicht-Übereinstimmung von Kontoinhaber oder Kreditkarteninhaber mit dem bei der Anmeldung angegebenen Namen des Nutzers ergeben, die Kontenverbindung trotz erfolgter Validitätsprüfung nicht existieren, das Konto keine ausreichende Deckung aufweisen oder das Kontenlimit überschritten sein, so wird die Beschwerdegegnerin von ihrer Bank unverzüglich informiert und das weitere Altersverifikationsverfahren ebenfalls abgebrochen. Durch die übliche Postlaufzeit ist beim Versand der Brief-PIN gewährleistet, dass Unregelmäßigkeiten in der Zahlungsabwicklung (welche auf einen nichtberechtigten und ggf. minderjährigen Nutzer hinweisen könnten) noch vor In-Empfangnahme der Brief-PIN durch den Besteller aufgedeckt werden und in einem solchen Fall das Freischaltverfahren abgebrochen wird.

Der Abgleich des Namens des Kontoinhabers bietet für sich alleine zumindest eine relative Sicherheit dafür, dass die Zahlungsabwicklung von einem Erwachsenen herrührt. Eine wirkliche Gewähr für eine geschlossene Benutzergruppe bietet dies allein jedoch nicht. Das

ist jedoch wegen des oben beschriebenen Zusammenspiels der einzelnen Kontrollmechanismen auch nicht notwendig.

Brief-PIN mittels Einschreiben „eigenhändig“

Innerhalb von vier Wochen kann der Nutzer grundsätzlich nur eine einzige Brief-PIN beauftragen. Damit wird unterbunden, dass ein ggf. minderjähriges Haushaltsmitglied mehrere Briefe aktiviert in der Hoffnung, im elterlichen Haushalt zumindest einen der Briefe abzufangen.

Darüber hinaus ist die mittels Einschreiben „eigenhändig“ zugestellte Brief-PIN nur einmalig zu verwenden. Der Nutzer muss sich zur Freischaltung zunächst mit seinem (getrennt von der Brief-PIN in der Begrüßungsmail von HIJKLMN erhaltenen) Usernamen und Passwort auf der Internetseite der Beschwerdegegnerin autorisieren und anschließend zur Freischaltung des Bereichs der geschlossenen Benutzergruppe die erhaltene 7-stellige Brief-PIN eingeben, wobei lediglich vier Fehlversuche bei der Eingabe der PIN zulässig sind. Nach dem fünften Fehlversuch wird dem Nutzer eine neue Brief-PIN wiederum per Einschreiben „eigenhändig“ zugestellt. Auf diese Weise kann angesichts der mit der erneuten Zusendung verbundenen Postlaufzeiten mit hinreichender Sicherheit ausgeschlossen werden, dass durch einen Unberechtigten und ggf. Minderjährigen selbst bei Kenntnis von Username und Passwort mittels bloßen Ausprobierens verschiedener Buchstaben-/Zahlenkombinationen die richtige PIN erraten sowie mittels automatisierter Passwortprogramme durchgespielt oder errechnet wird.

Bevollmächtigung von Minderjährigen bei der Übergabe der Brief-PIN mittels Einschreiben „eigenhändig“

Zwar könnten Probleme dahingehend auftreten, dass einem Minderjährigen als Bevollmächtigten (vgl. § 165 BGB) das Einschreiben „eigenhändig“ dennoch ausgehändigt wird.

Das Einschreiben „eigenhändig“ der Beschwerdegegnerin ist allerdings neutral gestaltet, so dass es lediglich die 7-stellige Brief-PIN enthält ohne Angabe der entsprechenden Internet-URL, über welche die Inhalte abrufbar sind sowie ohne Angabe von Username und Passworten, deren weitere Kenntnis unbedingte Voraussetzung des Zugriffs auf die Inhalte ist. Auf diese Weise wird gewährleistet, dass ein z.B. im Haushalt lebender Minderjähriger oder eine sonstige Person, die nach Übergabe des Einschreibens von dessen Inhalt Kenntnis nehmen sollte oder an welche das Einschreiben als Bevollmächtigten übergeben

wurde allein mit der Freischalt-PIN keinen Zugang in die geschlossene Benutzergruppe erhalten kann.

cc) Dritte Variante: Altersverifizierung mittels Konto-Pin ausreichend

Das von der Beschwerdegegnerin als dritte Variante eingesetzte Konto-PIN-Verfahren ist in seiner konkreten Ausgestaltung zum Nachweis der Volljährigkeit auf der Stufe der Identifizierung ebenfalls als hinreichend anzusehen: Das Zusammenspiel und Ineinandergreifen mehrerer Kontrollroutinen führt - aufgrund des Rückgriffs auf die Kontrollroutinen des soeben beschriebenen Verfahrens zum Schufa-Datenabgleich (s.o.) - dazu, dass auch hier ein „Sicherstellen“ iSd § 4 Abs. 2 S. 2 JMStV anzunehmen ist.

Der User wird auch im Konto-PIN-Verfahren anhand seiner Personen- und Adressdaten eindeutig in der Datenbank der Schufa Holding AG identifiziert. Das vom User eingegebene Geburtsdatum wird mit dem Datensatz der Schufa Holding AG verglichen. Nur wenn der Wert exakt übereinstimmt und der User das 18. Lebensjahr vollendet hat, kann das Verfahren fortgesetzt werden.

In einem zweiten Schritt wird dem User von dem unbedingt auf seinen Namen lautenden persönlichen Konto ein Betrag abgebucht (dies ist beim Abo-Verfahren in der Regel der erste Monatsbeitrag), in dessen Überweisungsvermerk ein eindeutiger und einmaliger Freischalt-PIN für die geschlossene Benutzergruppe enthalten ist.

Das Konto-PIN-Verfahren unterscheidet sich nur in diesem zweiten Schritt (also durch die Art der Übermittlung der PIN) von dem o.g. Brief-PIN-Verfahren:

- Ebenso wie beim Brief-PIN-Verfahren (dort: Verzögerung wg. der Postlaufzeit, s.o.) wird im Konto-PIN-Verfahren durch die Zahlungsabwicklungsmodalität (Abbuchung in der Regel erst mit Zeitverzögerung) gewährleistet, dass in der Zwischenzeit Abbuchungsaufträge bei Nicht-Übereinstimmung von angegebenem und tatsächlichem Kontoinhaber bankseitig storniert werden und daher auch eine im Überweisungsvermerk übermittelte Freischalt-PIN nicht auf einem Kontoauszug eines unberechtigt (d.h. nicht durch Schufa-Daten bestätigten) belasteten Kontoinhabers erscheinen kann.

- Bei erfolgreicher und berechtigter Abbuchung gegenüber dem zuvor durch die Schufa-Datenbank als volljährig identifizierten tatsächlichen Inhaber der belasteten Kontenverbindung ist jedoch ebenfalls davon auszugehen, dass nur dieser selbst als erster und persönlich über seinen entweder online abgerufenen oder bei der Bank am Schalter bzw. mittels Kontoauszugsdrucker erhaltenen oder per Brief zugesendeten

Kontoauszug Kenntnis von der Konto-PIN nehmen kann. Denn Zugang zum Kontoauszug eines Kontoeigners hat in der Regel nur der Kontoinhaber selbst via Online-Banking (mit geschützten Login-Daten, die aufgrund des hohen Missbrauchs-Risikos in aller Regel nicht an Dritte weitergegeben werden) oder unter Nutzung der haptischen Kontokarte. Eine freiwillige Weitergabe der Kontokarte an (minderjährige) Dritte ist wegen der meist damit verbundenen Einsatzmöglichkeit für den bargeldlosen Zahlungsverkehr (häufig ohne PIN, stattdessen nur mit Unterschrift; bei einer Kontokarte mit zusätzlicher Geldkartenfunktion sogar völlig ohne PIN oder Unterschrift) für den volljährigen Kontoeigner höchst risikoreich und dürfte daher in aller Regel auszuschließen sein.

- Aber auch eine vom volljährigen Kontoinhaber nicht autorisierte Kenntnisverschaffung von Kontoauszugs-Inhalten durch einen Minderjährigen dürfte auszuschließen sein bzw. würde beim Minderjährigen nicht zum gewünschten Erfolg führen. Denn anders als bei irgendeinem vom Minderjährigen mit den Daten des Erwachsenen angeforderten und dann „abgefangenen“ - nicht eigenhändigen - Brief, dessen Empfang z.B. durch anschließendes Wegwerfen leicht „vertuscht“ werden kann, würde ein solches Abfangen eines Kontoauszugs durch einen unberechtigten (minderjährigen) Dritten wegen der zwingend fortlaufenden Nummerierung der Kontoauszüge und der steuerlichen Bedeutung der ausgedruckten Belege sofort auffallen. Schon aus diesem Grunde dürften die meisten (volljährigen) Kontoinhaber ein gesteigertes Interesse an der persönlichen, rechtzeitigen und lückenlosen Kenntnis aller ihrer Kontoauszüge sowie an deren sorgfältiger Aufbewahrung haben.
- Sollte dennoch ein Minderjähriger in den Besitz eines Kontoauszugs gelangen und damit Kenntnis der bis dato noch nicht verbrauchten einmaligen Konto-PIN erhalten, so ist auch hier - wie bei der Brief-PIN - durch die neutrale Gestaltung (lediglich 7-stellige Konto-PIN ohne Angabe der entsprechenden Internet-URL sowie ohne Angabe von Username und Passwörtern, deren weitere Kenntnis unbedingte Voraussetzung des Zugriffs auf die Inhalte ist) gewährleistet, dass der Minderjährige allein mit der Freischalt-PIN nichts anfangen kann.

dd) Vierte Variante: Altersverifizierung mittels Geldkarten-Check ausreichend

Auch das von der Beschwerdegegnerin als vierte Variante eingesetzte Verfahren mittels Geldkarten-Check ist in seiner konkreten Ausgestaltung zum Nachweis der Volljährigkeit auf der Stufe der Identifizierung als hinreichend anzusehen, soweit es durch weitere von der Beschwerdegegnerin eingesetzte Maßnahmen auf der Stufe der Authentifizierung ergänzt wird. Der User wird nach erfolgter Anmeldung gebeten, seine Geldkarte mit Altersmerkmal

in ein Lesegerät seines Computers einzuschieben. Nur wenn das Altersmerkmal „älter als 18 Jahre“ zeigt, wird der User für die geschlossene Benutzergruppe freigeschaltet.

Bei der Abwicklung der Altersverifikation via Geldkarte bedient sich die Beschwerdegegnerin des Moduls „fun SmartPay AVS“ der fun communications GmbH, welches von der KJM als positiv bewertet wurde (vgl. Pressemitteilung der KJM v. 22.09.2005). Dieses sieht keine eigene Identifizierung vor, sondern greift auf eine bereits erfolgte Face-to-Face-Kontrolle bei der Eröffnung eines Bankkontos zurück und nutzt das Jugendschutzmerkmal der GeldKarte der deutschen Kreditwirtschaft. Die kontogebundenen ec-, Bank-, und Sparkassenkarten sind in ihrer aktuellen Version mit Chips (Geldkarte) ausgestattet, die den Bankkunden durch ein zusätzliches Altersmerkmal zur Nutzung verschiedener Funktionen autorisieren können und in ihrer Funktion als elektronische Geldbörse auch ohne zusätzliche PIN oder Unterschrift zu monetären Transaktionen berechtigen. Da die Weitergabe einer solchen Karte an (minderjährige) Dritte wegen des damit verbundenen finanziellen Risikos sehr unwahrscheinlich ist, geht hiesiger Beschwerdeausschuss - in Übereinstimmung mit der Ansicht der KJM - davon aus, dass die bereits bei den Banken erfolgte Altersüberprüfung ausreicht.

Darüber hinaus erfolgt bei dem System der Beschwerdegegnerin (über die unten genannten und dort näher beschriebenen Sicherungsmaßnahmen insbes. die sog. Einmal-Cookies auf der Stufe der Authentifizierung hinausgehend) nach der Verifizierung über das Altersmerkmal der Geldkarte ein automatisierter regelmäßiger „Time-Out“, so dass ein solcher User seine weitere Zugangsberechtigung zur Geschlossenen Benutzergruppe in regelmäßigen Zeitabständen durch erneute Verifikation über die Geldkarte nach o.g. Ablaufschema nachweisen muss. Andernfalls erhält er keinen weiteren Zugang zur geschlossenen Benutzergruppe.

ee) Fünfte Variante: Altersverifizierung mittels Webcam-Check nicht ausreichend

Das von der Beschwerdegegnerin als fünfte Variante eingesetzte Verfahren mittels **Webcam-Check** ist in seiner konkreten Ausgestaltung zum Nachweis der Volljährigkeit auf der Stufe der Identifizierung hingegen **nicht** als hinreichend anzusehen: Ein „Sicherstellen“ i.S.d. § 4 Abs. 2 S. 2 JMStV ist hier derzeit nicht anzunehmen.

Derzeit ist es möglich, dass der User nach erfolgter Anmeldung und Eingabe seiner Personendaten sowie des Geburtsdatums sich im Chat via Live-Webcam (Bewegtbild) einem speziell geschulten Support-Mitarbeiter zeigt, der das Alter des Gezeigten abschätzt

sowie sich in Zweifelsfällen hinsichtlich des Alters (als interne Maßgabe der Beschwerdegegnerin gelten hier unter bzw. „ab ca. 25 Jahre“) oder bei sonstigen Zweifeln anhand eines in die Webcam gehaltenen erkennbaren gültigen amtlichen Lichtbildausweisdokuments die Richtigkeit der eingegebenen Daten bestätigen lässt. Bei weiteren Zweifeln (z.B. Verdacht auf ein möglicherweise vorbereitetes Video mit Darstellung einer - anderen - erwachsenen Person) wird der User durch den Support-Mitarbeiter über den Chat z.B. aufgefordert, eine bestimmte vom Support-Mitarbeiter kurzfristig vorgegebene Bewegung vor der Webcam zu zeigen. Eine Freisaltung erfolgt dann nach vom Support-Mitarbeiter für ausreichend erachteter Verifikation ohne weitere Zusendung einer PIN o.ä. direkt durch den Support-Mitarbeiter.

Alle sowohl von der FSM als auch von der KJM in bisherigen Entscheidungen für Telemedien akzeptierten Identifikationsmaßnahmen zum Altersnachweis und damit zur Sicherung einer geschlossenen Benutzergruppe, welche nicht durch einen direkten echten persönlichen Kontakt zwischen Anbieter und Nutzer zustande kommen, basieren direkt oder indirekt auf der **ausnahmslosen** und zwingenden Überprüfung amtlicher Ausweisdokumente mit Lichtbild. Auch der hiesige Beschwerdeausschuss gelangt zu der Überzeugung, dass nach derzeitigem Stand der Technik und insbesondere beim Webcam-Check (der ja ebenfalls nicht auf einem echten persönlichen Kontakt zwischen Anbieter basiert, sondern auf elektronische Hilfsmittel zurückgreift) von diesem Erfordernis nicht abgewichen werden kann.

Das von der Beschwerdegegnerin durchgeführte Verfahren genügt diesen Anforderungen in seiner konkreten Durchführung derzeit allerdings nicht: Denn eine Überprüfung anhand eines amtlichen gültigen Ausweisdokuments findet derzeit nicht ausnahmslos statt, sondern lediglich in den oben beschriebenen „Zweifelsfällen“. Dadurch ist nicht mit hinreichender Sicherheit gewährleistet, dass der tatsächliche Leistungsempfänger (User) auch genau diejenige (scheinbar) erwachsene Person ist, die sich im Webcam-Chat zeigt, deren Daten gleichzeitig zum Aufbau einer in der Regel längerfristigen/dauerhaften Vertragsbeziehung aufgenommen wurden und auf mehr als nur eine einmalige Leistungserbringung zum Zeitpunkt des Webcam-Chats seitens des Anbieters abzielen. Genau dies sollte in seiner Kombination in Telemedien durch ein wirksames Altersverifikationssystem bei den von der Beschwerdegegnerin verbreiteten Angeboten allerdings sichergestellt werden.

Der von der Beschwerdegegnerin vorgetragene Vergleich mit der Offline-Praxis z.B. in Ladengeschäften, bei dem eine Alterskontrolle anhand eines amtlichen Ausweisdokuments ebenfalls nur in Zweifelsfällen stattfindet, vermag daher ebenfalls nicht zu überzeugen. Denn im Ladengeschäft wird in der Mehrzahl nur ein einmaliger Zugang zu jugendschutzrelevanten Angeboten (z.B. Verkauf pornografischen Materials oder Konsum

eines Pornofilms während der Dauer des Aufenthalts im Ladengeschäft) und auch hinreichend sicher nur gegenüber derjenigen erkennbar erwachsenen Person gewährt, die leibhaftig im Moment der Leistungserbringung dem Anbieter/Ladenpersonal gegenübersteht und jedenfalls für die Dauer der Vertragsbeziehung eindeutig als volljährig identifiziert werden kann. Manipulationen gegenüber dem Anbieter/Ladenpersonal von Seiten des Kunden (z.B. durch heimliches „Auswechseln“ des sicher Erwachsenen gegen einen Minderjährigen im Moment des anschließenden Leistungsbezugs) können offline insoweit mit ausreichender Sicherheit rechtzeitig vorher erkannt und durch anwesendes Ladenpersonal ausgeschlossen werden.

Anders als im Offline-Geschäftsverkehr kann eine - nicht nur denkbare, sondern auch höchst wahrscheinliche - Manipulation beim Zustandekommen einer auf Dauer angelegten **Online-Vertragsbeziehung** nicht mit hinreichender Sicherheit ausgeschlossen werden. Die von der Beschwerdegegnerin primäre Abgrenzung von Zweifelsfällen lediglich „unter/ab ca. 25 Jahre“ ist insoweit nicht wirklich hilfreich, da auf diese Weise nicht ausreichend sichergestellt ist, dass die Person in der Webcam auch tatsächlich zu den sonstigen Anmeldedaten passt und damit der wirkliche volljährige Leistungsempfänger sowie z.B. der in den Anmeldedaten aufgeführte Kontoinhaber ist. Dies kann nur durch einen zusätzlichen **ausnahmslosen** (und nicht von der vordergründigen Webcam-Darstellung durch den

Support-Mitarbeiter möglicherweise nur vermuteten) Abgleich der dort gezeigten Person mit einem Lichtbild sowie den sonstigen persönlichen Angaben in einem gültigen amtlichen Ausweisdokument hinreichend sicher erfolgen. Schon aus diesem Grund ist ein „Sicherstellen“ iSd § 4 Abs. 2 S. 2 JMStV hier derzeit nicht anzunehmen.

Ob darüber hinaus die sonstigen seitens der Beschwerdegegnerin aufgestellten Maßgaben gegenüber ihren Support-Mitarbeitern beim Webcam-Check ausreichend iSd § 4 Abs. 2 S. 2 JMStV sind (z.B. hinsichtlich zulässiger Bildqualität beim Einsatz und der Durchführung des Webcam-Checks, Erkennbarkeit und Überprüfung genau vorgegebener dem Ausweis entnehmbarer Daten, evtl. besondere Anforderungen an die Erkennbarkeit besonderer holographischer Merkmale und Dokumentation bei bestimmten Nutzer-/Altersgruppen, Prüfung auf mögliche Fälschungen, evtl. detaillierte schriftliche Richtlinien zur Durchführung des Webcam-Checks sowie ausdrückliche und schriftliche Verpflichtung auf deren exakte Einhaltung durch Support-Mitarbeiter, evtl. deren regelmäßige Kontrolle usw.), muss an dieser Stelle daher nicht mehr entschieden werden.

b) Zweite Stufe: Authentifizierung zur Verhinderung der massenhaften Weitergabe der Zugangsdaten ausreichend

Auf der zweiten Stufe muss durch ein ausreichendes AVS zusätzlich gewährleistet werden, dass nach Bekanntgabe/Übersendung und Eingabe der Freischalt-PIN (im Konto-Pin- und Brief-PIN-Verfahren) oder nach Freischaltung (im Post-Ident-Verfahren bzw. beim Geldkarten-Check) keine - jedenfalls keine massenweise - Weiterverbreitung der Zugangsdaten beispielsweise an Minderjährige erfolgen kann.

Bei den von der Beschwerdegegnerin nach ausreichender Erstidentifizierung (s.o. aa) bis dd)) eingesetzten Sicherungsmaßnahmen ist eine massenweise Weitergabe der Nutzungsdaten des berechtigten Erwachsenen an andere (minderjährige) Nutzer nicht zu befürchten, da insbesondere das damit verbundene Kostenrisiko für den Nutzer teils unübersehbar hoch ist und da eine Verbreitung sowie Parallelnutzung (bei einer Nutzung über verschiedene IP-Adressen) auch durch eine Kombination technischer Sicherungsmaßnahmen wirksam ausgeschlossen wird. Die Authentifizierungsstufe erfüllt damit sowohl die Anforderungen der FSM als auch die der Landesmedienanstalten nach Ziff. 5.1 der Jugendschutzrichtlinie:

Allgemeine Geschäftsbedingungen

Das Verbot der Weitergabe der Zugangsdaten insbes. an Minderjährige in den Nutzungsbedingungen des integrierten Zahlungssystems HIJKLMN (sowie teilweise noch eingesetzten ABCDEFG) stellt allein allerdings noch nicht einen solchen Schutz dar, da die sich daran knüpfenden Rechtsfolgen lediglich zivilrechtlicher Natur sind, jedoch keinen Einfluss auf den öffentlich-rechtlichen Jugendschutz gem. § 4 Abs. 2 JMStV haben.

Beeinträchtigungen der virtuellen Identität des Berechtigten

Nach Auffassung der Beschwerdegegnerin soll die unerwünschte Preisgabe der Privatsphäre, die mit der Weitergabe der Zugangsdaten verbunden ist (Einsichtnahmemöglichkeit in interne Messages, Buddy-Lists und deren Veränderungsmöglichkeiten), von einer solchen Weitergabe abhalten. Ein wirksames Sicherungsmittel zur Aufrechterhaltung einer geschlossenen Benutzergruppe liegt allein in der Gefahr der Beeinträchtigung der virtuellen Identität aber ebenfalls nicht, da es für einzelne Nutzer unerheblich oder vielleicht sogar erwünscht sein mag, andere an ihrer virtuellen Identität zu beteiligen.

Technische Schutzmaßnahmen

Die von der Beschwerdegegnerin eingesetzten technischen Schutzmaßnahmen bieten bereits eine recht hohe Hürde insbes. gegen eine massenhafte Verbreitung der Zugangsdaten an ggf. Minderjährige:

Parallelnutzungen (mit zwei verschiedenen IP-Adressen zur gleichen Zeit) unter demselben Usernamen werden technisch ausgeschlossen. Auch die Funktion „Auto-Vervollständigen“ ist auf den Seiten der Beschwerdegegnerin deaktiviert, so dass ein Minderjähriger sich über einen zuvor auf den Seiten der Beschwerdegegnerin angemeldeten Computer nicht einloggen kann, wenn er nicht den genauen Usernamen und das exakte Passwort kennt. Direktaufrufe von Bildlinks oder Videostreams werden ohne ordnungsgemäßes Login ebenso unterbunden wie sonstige Versuche, eine bekannt gewordene URL des Bereich der geschlossenen Benutzergruppe direkt ohne vorherigen ordnungsgemäßen Login aufzurufen.

Darüber hinaus wird dem Nutzer nach erfolgter Freischaltung auf der Website der Beschwerdegegnerin bei der ersten Nutzung ein Website-Cookie gesetzt.

Bei erneutem Login über den Usernamen und das Passwort wird die Gültigkeit dieses zuletzt gesetzten sog. „Einmal-Cookies“ mit der Datenbank der Beschwerdegegnerin abgeglichen und bei Übereinstimmung durch einen neuen Einmal-Cookie ersetzt, anschließend kann der Nutzer den Bereich der geschlossenen Benutzergruppe betreten.

Dieser sog. „Einmal-Cookie“ erlaubt es, den Nutzercomputer bei der Wiederkehr auf die gleiche Website wiederzuerkennen und mittels Username sowie Passwort den abermaligen Zugriff auf Inhalte des Bereichs der geschlossenen Benutzergruppe zu gestatten. Gleichzeitig wird eine mögliche massenhafte Weiterverbreitung des Cookies (z.B. mittels Cookie-Export) und damit eine massenhafte Zugriffsmöglichkeit verhindert, da nach einer Weitergabe des Cookies an einen anderen Rechner jeweils nur der erste den Cookie nutzende Computer sich mit dem Usernamen und dem Passwort einloggen, den gültigen Wert verändern und durch einen neuen gültigen Cookie ersetzen kann. Auf diese Weise wird sichergestellt, dass immer nur ein Nutzer unter demselben Usernamen und Passwort mittels gültigen Cookies Zugang zum Bereich der geschlossenen Benutzergruppe der Beschwerdegegnerin erhalten kann.

Insgesamt kann der Zugang auf bis zu drei Computern installiert werden, die jeweils mit einem Einmal-Cookie ausgestattet werden. Jeder weitere Zugang/Rechner/Browser kann nur über den Usernamen mit dem Masterpasswort (zum Kostenrisiko bei dessen Weiterverbreitung: vgl. unten) sowie in Verbindung mit einer unigen 7-stelligen Mail-TAN frei geschaltet werden (welche bei der Anmeldung eines weiteren bisher nicht registrierten Browsers automatisiert an die bei der Erstanmeldung angegebene gültige E-Mailadresse gesendet wird), wobei bei letzterer lediglich 5 Fehleingaben erlaubt sind und einen anschließendem Timeout zur Folge haben. Ein weiterer (vierter) nutzender Computer/Browser deaktiviert auf diese Weise jeweils ersten registrierten Browser. Eine

massenhafte Verbreitung durch Weitergabe von Zugangsdaten ist daher ausgeschlossen. Eine Parallelnutzung ist - wie beschrieben - technisch ebenfalls ausgeschlossen.

Zum Einloggen in den Bereich der geschlossenen Benutzergruppe über einen weiteren Computer, auf dem nicht bereits der gerade gültige Cookie abgelegt ist, muss der Nutzer sich daher zusätzlich mittels Mail-TAN sowie mittels seines Master-Passwort authentifizieren, dessen Weitergabe allerdings aufgrund der integrierten Bezahlungsfunktion für den Nutzer mit einem hohen finanziellen Risiko behaftet ist (vgl. unten). Hat der Nutzer seinen Usernamen sowie das Passwort an einen oder gar mehrere (minderjährige) Dritte

weitergegeben, so können diese sich auf ihren Computern ohne zusätzliche Kenntnis des Masterpassworts sowie der unigen Mail-TAN nicht in den Bereich der geschlossenen Benutzergruppe der Beschwerdegegnerin einloggen.

Finanzielle Risiken bei der Weitergabe der Login-Daten

Wie bei vergleichbaren technischen Schutzmaßnahmen ist auch hier nicht ausgeschlossen, dass sich Minderjährige die Zugangsdaten inkl. Master-Passwort eigenmächtig beschaffen oder dass sie ihnen von einem berechtigten registrierten Nutzer möglicherweise genannt werden.

Um diese Gefahr der Weitergabe der Zugangsdaten weiter zu reduzieren, ist in das System die Bezahlungsfunktion HIJKLMN (teilweise auch noch ABCDEFG) integriert. Gibt ein berechtigter Nutzer seinen Zugang (insbes. das Master-Passwort, mittels dessen ein weiterer Computer überhaupt erst für die Nutzung des Systems registriert werden kann) weiter, ist dies mit einem erheblichen Kostenrisiko für ihn verbunden, da hochpreisige Dienstleistungen von dem (minderjährigen) Nutzer auf Kosten des Weitergebenden in Anspruch genommen werden können.

Aufgrund des teilweise unkalkulierbar hohen Kostenrisikos in seiner Sphäre kann davon ausgegangen werden, dass ein berechtigter registrierter Nutzer das zur Neuregistrierung eines weiteren Rechners erforderliche Master-Passwort sowie die erhaltene Mail-TAN nicht weitergeben wird.

Die Gefahr einer (massenhaften) Weitergabe von Zugangsdaten wird also durch die integrierten Bezahlungsfunktionen zusätzlich minimiert.

c) Ergebnis

Das Altersverifikationssystem der Beschwerdegegnerin entspricht in vier oben bewerteten nunmehr eingesetzten Varianten sowohl hinsichtlich der Verifikation bei der Anmeldung als auch hinsichtlich der Authentifizierung bei jedem Nutzungsvorgang den Erfordernissen des § 4 Abs. 2 S. 2 JMStV und den Erfordernissen der Jugendschutzrichtlinie der Landesmedienanstalten. Der ebenfalls bewertete von der Beschwerdegegnerin eingesetzte Webcam-Check entspricht diesen Erfordernissen aus den oben genannten Gründen nicht.

6. Abhilfeaufforderung

Die Beschwerdegegnerin wird daher aufgefordert, binnen einer Frist von 14 Tagen ab Bekanntgabe dieser Entscheidung

- den Webcam-Check in seiner bisherigen Version als Identifikationsmaßnahme für alle ihre Angebote nicht mehr einzusetzen
- bei Beibehaltung eines Webcam-Checks in verbesserter Version für alle ihre Angebote eine Sicherstellung der geschlossenen Benutzergruppe gemäß den Voraussetzungen des § 4 Abs. 2 S. 2 JMStV zu gewährleisten.
- für alle ihre Angebote nur eine solche Alterskontrolle zu installieren / anzubieten, die den oben genannten Voraussetzungen entspricht und durch welche eine Abrufmöglichkeit von pornographischen und offensichtlich schwer entwicklungsgefährdenden Inhalten durch Minderjährige sicher ausgeschlossen wird.

Die Beschwerdegegnerin wird aus diesem Grunde insbesondere auch aufgefordert, binnen der o.g. Frist von 14 Tagen ab Bekanntgabe dieser Entscheidung auch ihre sonstigen Bereiche (neben den Angeboten unter <http://www.de>, <http://www.de>, <http://www.de>, <http://www.de> auch über folgende URLs abrufbare Angebote: <http://www.de>, <http://www.de>, <http://www.de>, <http://www.de> ; sowie die weiteren von XY GmbH nach den Vorschriften des JMStV sowie des Teledienstegesetzes (TDG) zu verantwortenden Angebote) in eigener Verantwortung auf Jugendschutzrelevanz hin zu kontrollieren und umgehend den gesetzlichen Vorgaben des Jugendmedienschutz-Staatsvertrags entsprechende wirksame Maßnahmen zur Einschränkung des Zugriffs Minderjähriger nach den o.g. Vorgaben durch Installierung eines ausreichenden Altersverifikationssystems zu ergreifen.

Anmerkung

Die Beschwerdegegnerin hat im Wege der Abhilfe die bis dahin große Anzahl vorhandener (und oftmals nicht ausreichender) Alterverifikationsverfahren reduziert, umfassend verbessert und (mit einer Ausnahme) nach Auffassung des Beschwerdeausschusses den gesetzlichen Vorgaben ausreichend angepasst. Um nachhaltig in allen Angeboten den nunmehr erreichten Standard zu gewährleisten, scheint es uns empfehlenswert, die Anzahl

der Varianten weiter zu verringern und den Zugang zu den geschlossenen Benutzergruppen in allen Angeboten möglichst einheitlich zu regeln.

gez.

XY
(Vorsitzende des Beschwerdeausschusses)

Berlin, den x.y.2006

XX
im Auftrag des Vorsitzenden des FSM Beschwerdeausschusses