die medienanstalten

BLM, Heinrich-Lübke-Straße 27, 81737 München

Behörde für Inneres und Sport
der Freien und Hansestadt Hamburg
[redacted]
Amt für Innere Verwaltung und Planung
[redacted]Glücksspielaufsicht
Johanniswall 4
20095 Hamburg

- per Mail a[redacted]
und cc a[redacted]

KJM
Kommission für Jugendmedienschutz

[redacted]
Vorsitzender

c/o Bayerische Landeszentrale für neue Medien (BLM)
Heinrich-Lübke-Straße 27
81737 München

ALM GbR
Gemeinsame Geschäftsstelle
Friedrichstraße 60
10117 Berlin

Tel.: (030) 206 46 90 - 0
Fax: (030) 206 46 90 - 99
kjm@die-medienanstalten.de
www.kjm-online.de
www.die-medienanstalten.de

Stellungnahme zur Konzeptbeschreibung der LOTTO Hamburg GmbH im Hinblick auf die AVS-Anforderungen der KJM
(Ihr Schreiben über die Medienanstalt Hamburg /Schleswig-Holstein an die KJM-Stabsstelle vom 23.07.2013)

München, den 18.11.2013

Sehr geehrter H[redacted]

mit Schreiben vom 23.07.2013[1] baten Sie die Medienanstalt Hamburg /Schleswig-Holstein (MA HSH) um unterstützende Stellungnahme zu der Frage, ob das von der LOTTO Hamburg GmbH (LH) vorgesehene Konzept zur Sicherstellung des Ausschlusses von minderjährigen und gesperrten Spielern (vgl. § 4 Abs. 5 Nr. 1 GlüStV) den Anforderungen der KJM an die Kriterien zur Bewertung von Konzepten für Altersverifikationssysteme (AVS) als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV („AVS-Raster") entspricht.

Die MA HSH hat mit Schreiben vom 29.07.2013 die Stabsstelle der Kommission für Jugendmedienschutz (KJM) in Kenntnis gesetzt.[2]

[1] Vgl. Anlage D: „Amtshilfeersuchen von HH BIS an MA HSH vom 29.07.2013"
[2] Vgl. Anlage E: „Weiterleitung MA HSH_ Amtshilfe HH BIS_Lotto HH vom 29.07.2013"

Der Vorsitzende der KJM ist aufgrund der Bewertung der AG Telemedien vom 09.09.2013 auf Grundlage der vorgelegten Unterlagen der Ansicht, dass das von der LH vorgesehene Konzept (vgl. Anlagen B, C und F) zur Sicherstellung des Ausschlusses von minderjährigen und gesperrten Spielern (vgl. § 4 Abs. 5 Nr. 1 GlüStV) den Anforderungen der KJM an die Kriterien zur Bewertung von Konzepten für AVS als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV („AVS-Raster") entspricht.

Diese Stellungnahme beruht auf folgenden Überlegungen und Gründen:

1. Rechtslage

a) Regelungen zur geschlossenen Benutzergruppe gem. § 4 Abs. 2 S. 2 JMStV

Für die vorliegende Stellungnahme des Vorsitzenden der KJM und die Bewertung des Konzepts der LOTTO Hamburg GmbH (LH) wurden die Regelungen zur geschlossenen Benutzergruppe gem. § 4 Abs. 2 S. 2 JMStV zu Grunde gelegt:

Von Seiten des Anbieters ist für eine geschlossene Benutzergruppe sicherzustellen, dass bestimmte jugendgefährdende Angebote nur Erwachsenen zugänglich gemacht werden. Dies ist gemäß den Jugendschutzrichtlinien der Landesmedienanstalten[3] grundsätzlich durch zwei Schritte sicherzustellen: durch eine Volljährigkeitsprüfung, die über persönlichen Kontakt erfolgen muss, und durch eine Authentifizierung beim einzelnen Nutzungsvorgang.

Die Bewertung der vorgelegten Konzepte im Einzelfall erfolgt dabei auf der Grundlage eines von der KJM beschlossenen Kriterienrasters, welches die in § 4 Abs. 2 S. 2 JMStV und in den Jugendschutzrichtlinien der Landesmedienanstalten getroffenen Vorgaben weiter konkretisiert und ausdifferenziert. Die KJM hat zuletzt in ihrer Sitzung vom 19./20. September 2012 eine überarbeitete Version dieses Bewertungsrasters beschlossen, die nun auch maßgebend für die Stellungnahme der KJM zum Konzept der LH heranzuziehen war.[4]

---

[3] erstellt durch die KJM, vom 08./09.03.2005; in Kraft getreten am 02. Juni 2005.

[4] Vgl. Anlage A: Kriterien der KJM zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV („AVS-Raster)" mit Stand vom 11.09.2012

b) Internetanforderungen nach § 4 Abs. 5 GlüStV

Das Glücksspielkollegium der Länder hat in seiner Sitzung vom 11.09.2012 Eckpunkte zu den Internetanforderungen nach § 4 Abs. 5 GlüStV beschlossen, die im Erlaubnis- und Konzessionsverfahren bei der Prüfung der Internetanforderungen des Glücksspielstaatvertrages zugrunde gelegt werden sollen. Die Eckpunkte gehen von dem Grundsatz aus, dass die glücksspielrechtlichen Anforderungen **regelmäßig durch Verfahren erfüllt werden, die den Richtlinien der KJM entsprechen**. Antragsteller, die nicht von der KJM geprüfte Verfahren vorlegen, tragen die Darlegungslast, dass die Lösung in der Schutzwirkung gleichwertig ist. Über die Gleichwertigkeit wird im Erlaubnis- bzw. Konzessionsverfahren entschieden. Dabei kann die Erlaubnis- bzw. Konzessionsbehörde auf dem Weg der Amtshilfe eine Einschätzung der KJM einholen.

Aufgrund der jahrelangen Erfahrungen der KJM im Bereich der Bewertung von Altersverifikationskonzepten und nicht zuletzt um ein möglichst einheitliches Schutzniveau zu gewährleisten, wurde mit dem Vorsitz des Glücksspielkollegiums der Länder daher folgendes einheitliches Verfahren verabredet: Eine Einschätzung der KJM zu AVS-Konzepten für den Glücksspiel-Bereich kann und soll lediglich **im Rahmen der Amtshilfe gegenüber der jeweiligen Glücksspiel-Aufsichtsbehörde und auf deren Veranlassung hin** erfolgen, nicht jedoch als eigenständige Bewertung gegenüber dem Anbieter eines solchen Systems.

2. Begründung zur Stellungnahme des Vorsitzenden der KJM:

Die AG Telemedien der KJM hat sich mit der Anfrage der Behörde für Inneres und Sport der Freien und Hansestadt Hamburg und der von der LH vorgelegten Konzeptbeschreibung beschäftigt. Sie kam auf Basis der zur Einschätzung vorgelegten Unterlagen[5] zu dem Ergebnis, dass das Konzept der LH in der vorgelegten Version bei entsprechender Umsetzung als AVS-Konzept im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe für Erwachsene gem. § 4 Abs. 2 S. 2 JMStV geeignet ist. Aufgrund der Auswertung der zur Bewertung vorgelegten Unterlagen der LH kann mit ausreichender Sicherheit davon ausgegangen werden, dass durch dieses Konzept die AVS-Kriterien der KJM erfüllt werden.

[5] Vgl. Anlage B „Konzept Lotto Hamburg ‚Anlage 1' vom 17.06.2013",Anlage C „Konzept Lotto Hamburg ‚Anlage 2' vom 17.06.2013" und Anlage F „Konzeptergänzung von LH_SMS PIN am 24.09.2013"

a) JMStV als Bewertungsgrundlage:

Das o.g. Ergebnis der Einschätzung beruht auf folgender Bewertung nach den Vorgaben des JMStV und des AVS-Kriterienrasters der KJM wobei die glücksspielspezifischen Punkte des Konzepts der LH aus kompetenzrechtlichen Gründen nicht in die Prüfung mit einbezogen wurden:

b) Ebene der Identifizierung:

Die Identifizierung wird beim Konzept der LH über das von der KJM im September 2005 bereits positiv bewertete Modul „SCHUFA Identitäts-Check Jugendschutz" (mit Q-Bit) vorgenommen.

Daraufhin erfolgt eine Überprüfung der Übereinstimmung von Antragsteller und Kontoinhaber durch einen „SCHUFA-KontonummernCheck". Dadurch wird dem Antragsteller ein Bankkonto zugewiesen, auf das im nächsten Schritt der einmalige Aktivierungscode (im „Verwendungszweck" einer „1-Cent-Überweisung") geschickt werden kann.

c) Ebene der Authentifizierung:

Bei der Authentifizierung wird im Konzept der LH ein „SMS-PIN-Verfahren" eingesetzt, das laut Antragsteller dem von der KJM im Januar 2008 positiv bewerteten System der Lotterieverwaltung München entspricht.

Der Nutzer kann sich durch die Eingabe von Nutzernamen und Passwort in sein Kundenkonto einloggen. Transaktionen (Kauf/Abschluss von Spielverträgen oder Stammdatenänderungen) auf diesem Konto können nur durch Eingabe eines zeitlich begrenzten PINs vollzogen werden, der jeweils von der LH an eine registrierte Hardwarekomponente (stammdatenregistriertes Mobiltelefon) übermittelt wird.[6]

Zudem ist die Weitergabe der Zugangsdaten durch ein Kostenrisiko gesichert, da dem Nutzer bei Weitergabe seiner (Konto- und Benutzerkonto-) Daten erhebliche Kosten entstehen, sowie mögliche Gewinne entgehen könnten.

[6] Vgl. Anlage F „Konzeptergänzung von LH_SMS PIN am 24.09.2013"

[redacted]

3. Gesamtergebnis:

Der Vorsitzende der KJM kommt daher auf Basis der vorgelegten Unterlagen zu dem Ergebnis, dass das Konzept der LH als AVS-Konzept bei entsprechender Umsetzung im Sinne der KJM-Kriterien zur Sicherstellung einer geschlossenen Benutzergruppe für Erwachsene gem. § 4 Abs. 2 S. 2 JMStV geeignet ist.

Bei Rückfragen können Sie sich gerne an [redacted] wenden.

Mit freundlichen Grüßen

[redacted]

Anlagen:

a. Kriterien der KJM zur Bewertung von Konzepten für Altersverifikationssysteme als Elemente zur Sicherstellung geschlossener Benutzergruppen in Telemedien nach § 4 Abs. 2 S. 2 JMStV („AVS-Raster)"

b. Konzept Lotto Hamburg „Anlage 1" vom 17.06.2013

c. Konzept Lotto Hamburg „Anlage 2" vom 17.06.2013

d. Amtshilfeersuchen von HH BIS an MA HSH vom 29.07.2013

e. Weiterleitung MA HSH_ Amtshilfe HH BIS_Lotto HH vom 29.07.2013

f. Konzeptergänzung von LH_SMS PIN am 24.09.2013

Anlage 1 zum Schreiben vom 17.06.2013

Identifizierung von volljährigen Spielern im Internet Auftritt mittels Alters-Verifikations-System (AVS) bei Lotto Hamburg

I Identifizierung

Bei der Registrierung von Neukunden werden zunächst die Stammdaten der Kunden einschließlich der Mobilfunknummer und der Bankverbindungsdaten erfasst. Die Angabe/Nutzung einer Mobilfunknummer ist nur für genau ein Kundenkonto möglich (keine Mehrfachnutzung für weitere Kundenkonten).

Im ersten Teilschritt greifen wir für die geforderte Face-to-Face-Kontrolle auf bereits erfolgte Identifizierungen von Kreditinstituten zurück, die z. B. bei Kontoeröffnung mittels Personalausweis durchgeführt wurden: Die Stammdaten werden mittels **„Schufa-IdentitätsCheck Jugenschutz"** (SCHUFA-Q-Bit) geprüft. Dieser Teilprozess ist von der Kommission für Jugendmedienschutz bereits positiv bewertet und erleichtert die Erfüllung der gesetzlichen Anforderungen.

Bei positiv festgestellter volljähriger Identität des Antragstellers erfolgt im zweiten Teilschritt die Überprüfung der tatsächlichen Übereinstimmung von Antragsteller und Kontoinhaber durch den **„SCHUFA-KontonummernCheck"**. Durch den SCHUFA-KontonummernCheck werden die Personenstammdaten in Kombination mit der Bankleitzahl und der Kontonummer bzw. IBAN mit dem SCHUFA-Datenbestand abgeglichen. Hierzu werden Name, Vorname, Anschrift, Geburtsdatum, Bankverbindung sowie ggf. eine Voradresse geprüft.

Im dritten Teilschritt - bei positiv festgestellter tatsächlicher Identität von Antragsteller und Kontoinhaber (Kontowahrheit) - überweist LOTTO Hamburg dem Kunden 1 Cent auf dessen Kunden-Bankkonto mit Angabe eines einmaligen Aktivierungscodes im Verwendungszweck (**„1-Cent-Überweisung"**). Der Kunde kann nun seine Registrierung durch Eingabe dieses Aktivierungscodes fertigstellen.

Sofern ein der oben beschriebenen Teilschritte „SCHUFA JugendschutzCheck" (Teilschritt 1) oder „SCHUFA-KontonummernCheck" (Teilschritt 2) zu keiner positiven Feststellung der zu überprüfenden Daten führen, wird die online-Registrierung abgebrochen.

Alternativ kann der Kunde dann seine Identität und seine Volljährigkeit Face-to-Face in jeder LOTTO-Annahmestelle überprüfen lassen (**LOTTO-IDENT-VERFAHREN**). Hierzu werden die erfassten Angaben gegen einen amtlichen Lichtbildausweis des Kunden durch das LOTTO-Annahmestellenpersonal abgeglichen. Dieses Verfahren wurde von der Kommission für Jugendmedienschutz bereits in der Vergangenheit positiv bewertet (KJM-Entscheidung vom Juli 2007 zu Nordwest Lotto und Toto Hamburg).

II Authentifizierung

Der laufende Zugang zum Kundenkonto erfolgt durch Eingabe von Username und Passwort.

Für die laufende Authentifizierung zum Kauf / Abschluss von Spielverträgen sowie für Stammdatenänderungen wird das von der KJM bereits in der Vergangenheit positiv bewertete **SMS-PIN-Verfahren** genutzt.

Beim Anwendung des SMS-PIN-Verfahren sendet LOTTO Hamburg für den Abschluss jeder Spieltransaktion eine PIN-Nummer per SMS an die in den Stammdaten erfasste Mobilfunknummer des Kunden, die dieser zur Freigabe seiner Spieltransaktion eingeben muss (Entscheidung der KJM vom Januar 2008 zur Staatlichen Lotterieverwaltung München).

Die Änderung von Stammdaten durch Kunden (z. B. die Änderung der Kontoverbindung) erfordert von diesen ebenfalls eine Authentifizierung mittels SMS-PIN-Verfahren, um eine missbräuchliche Änderung zu unterbinden.

Das Weitergabe-Risiko der Zugangsdaten an unberechtigte Dritte ist darüber hinaus durch das hohe finanzielle Risiko des registrierten Kunden (Bankverbindung: Auslösung nicht rückzahlbarer Abbuchungen vom Giro- auf das Spielkonto, kostenpflichtiger Kauf von Spielaufträgen, Auszahlung von Gewinnen) zusätzlich hinreichend erschwert.

LOTTO HAMBURG®

Jugendmedienschutz bei LOTTO Hamburg

Vertrauenswürdige Altersverifikation für das Internet-Spielangebot von LOTTO Hamburg.

Verfahren einer positiven Auskunft durch die KJM

Hamburg, 11.03.2013

Unternehmensgegenstand

- LOTTO Hamburg ist die Staatliche Lotterie der Freien und Hansestadt Hamburg (FHH) und beauftragt, Staats- und sonstige Lotterien für die FHH durchzuführen.

  Die besondere gesellschaftspolitische Verantwortung für die Ordnung und Lenkung des Glücksspielmarktes ist Grundlage des Spielgeschäftes. Mit Begrenzung und Ordnung des Wettwesens wird die Spiel- und Wettsucht aktiv bekämpft und Begleitkriminalität auf ein nichtabwendbares Minimum begrenzt.

Vertriebswege

- LOTTO Hamburg bietet Lotterien und Sportwetten über drei Vertriebswege an:
  - terrestrisches Vertriebsnetz (über 400 Annahmestellen)
  - Abonnement
  - gewerbliche Spielevermittler
  - Internet

    Gemäß § 4 Abs. 4 Glücksspielstaatsvertrag (GlüStV) ist das Veranstalten und das Vermitteln öffentlicher Glücksspiele im Internet verboten. Die Länder können den Eigenvertrieb und die Vermittlung von Lotterien (...) im Internet erlauben (...). Die FHH hat LOTTO Hamburg diese Vertriebserlaubnis in 08/2012 erteilt.

Spielangebot im Internet

- Lotterien:
  - LOTTO 6aus49
  - Spiel77
  - Super6
  - KENO
  - plus5
  - GlücksSpirale

Sportwetten werden nicht über das Internet angeboten.

Identifizierung

- Online-**Registrierung** unter www.lotto-hh.de mit persönlichen Daten, Angabe einer Bankverbindung und Mobilfunknummer.
- Prüfung auf Volljährigkeit durch das SCHUFA-Modul „SCHUFA-JugenschutzCheck".
- Prüfung auf tatsächliche Identität von registrierter Person und Kontoinhaber durch das SCHUFA-Modul „SCHUFA-KontonummernCheck".
- 1-Cent-Überweisung mit Angabe eines einmaligen Aktivierungscodes im Verwendungstext
- Eingabe des Aktivierungscodes durch Kunden zur Freischaltung zum Abschluss von Spielaufträgen.

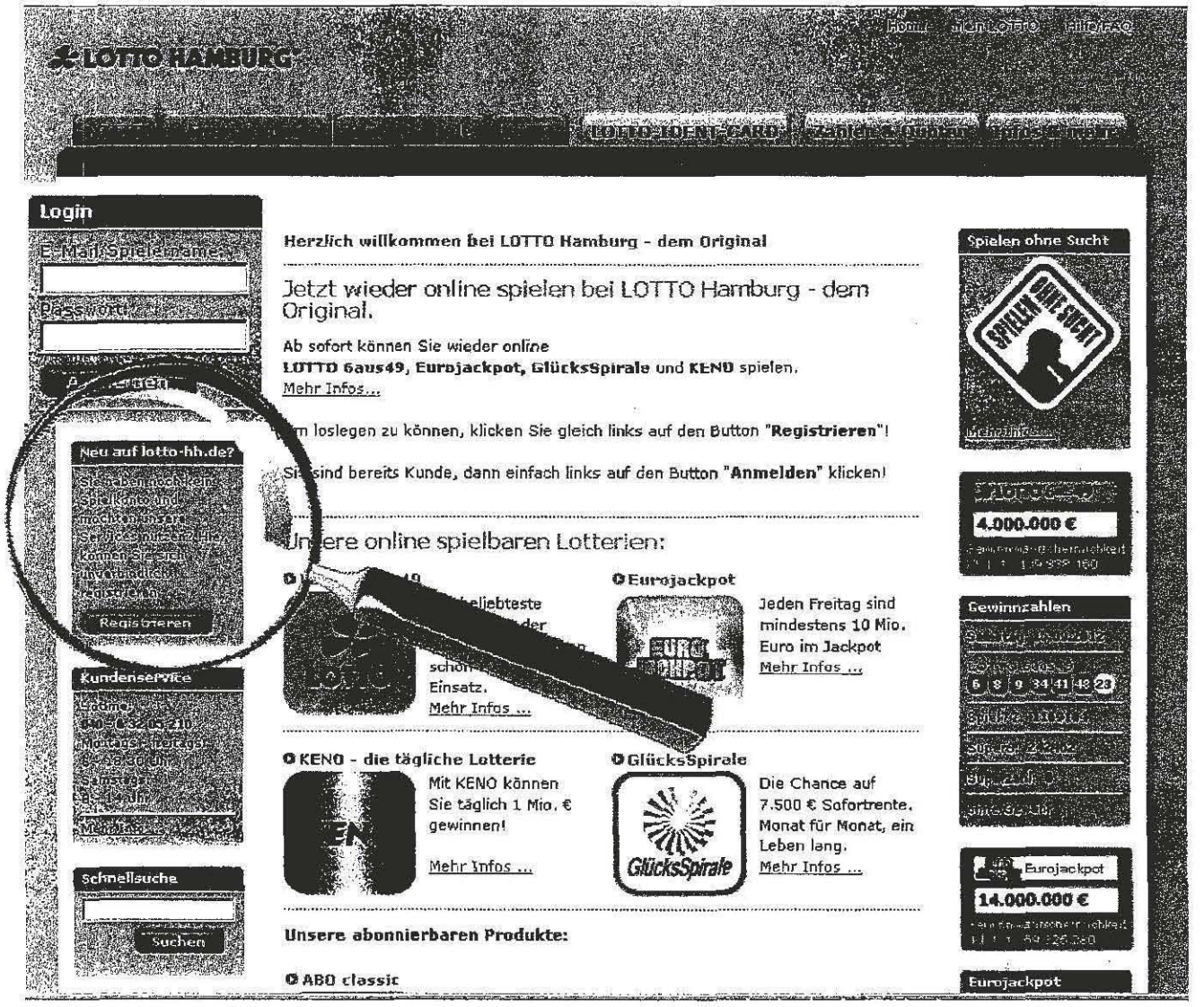
Authentifizierung

- Zugang zum Nutzerkonto durch Eingabe von Nutzername und Passwort.
- LOTTO-Spielaufträge müssen durch Eingabe einer per SMS zugesandten mTAN freigeschaltet werden.
- Veränderungen von Stammdaten, Bankverbindung und Mobilfunknummer müssen durch Eingabe der per SMS zugesandten mTAN freigeschaltet werden.

Identifizierung (1)

LOTTO HAMBURG

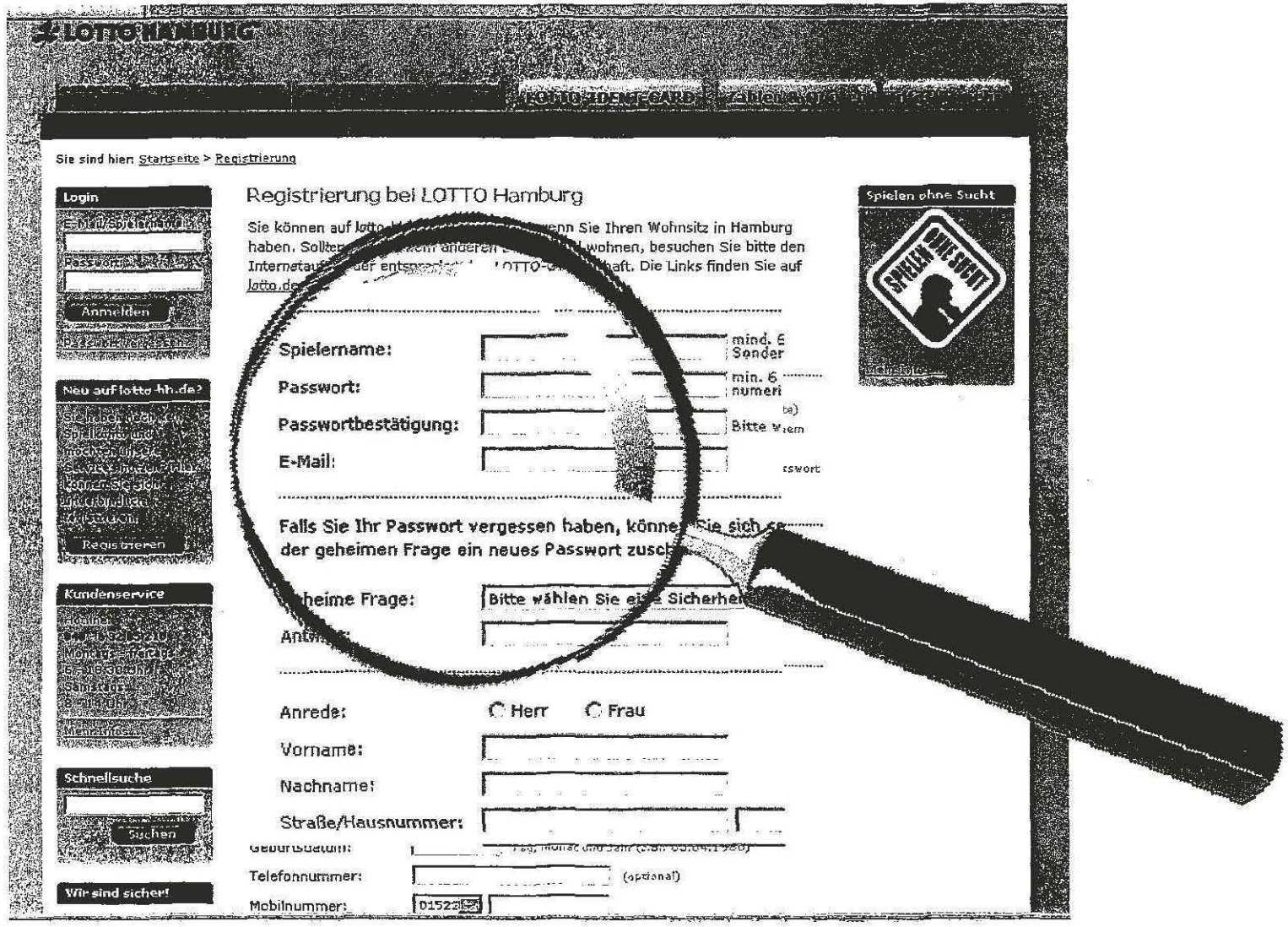
Start Online-Registrierung



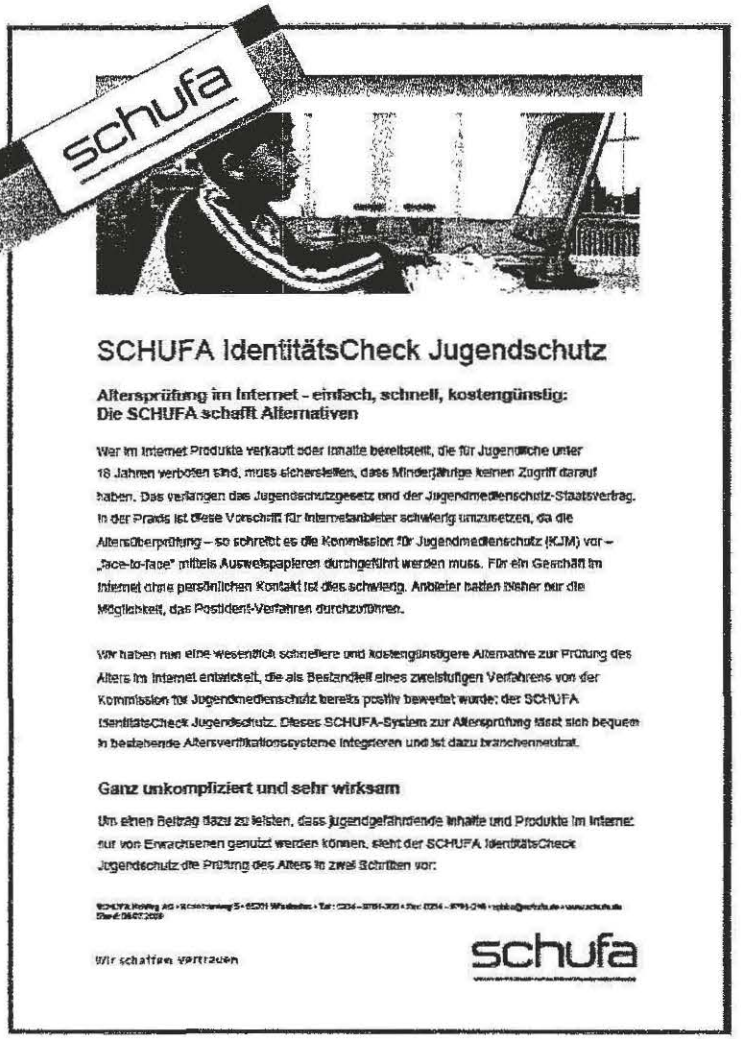
Identifizierung (2)

LOTTO HAMBURG

Online-Registrierung (Datenerfassung)



1. Teilprozess: SCHUFA-JugendschutzCheck



Im ersten Teilschritt greifen wir für die geforderte Face-to-Face-Kontrolle auf bereits erfolgte Identifizierungen von Kreditinstituten zurück, die z. B. bei Kontoeröffnung mittels Personalausweis durchgeführt wurden:

Die Stammdaten werden mittels **„Schufa-IdentitätsCheck Jugenschutz"** (SCHUFA-Q-Bit) geprüft.

Dieser Teilprozess ist ein von der Kommission für Jugendmedienschutz bereits positiv bewertet und erleichtert die Erfüllung der gesetzlichen Anforderungen.

2. Teilprozess: SCHUFA-KontonummernCheck

Bei positiv festgestellter volljähriger Identität des Antragstellers erfolgt im zweiten Teilschritt die Überprüfung der tatsächlichen Übereinstimmung von Antragsteller und Kontoinhaber durch den „**SCHUFA-KontonummernCheck**“.

Mit dem SCHUFA-KontonummernCheck werden die Personenstammdaten in Kombination mit der Bankleitzahl und der Kontonummer mit dem SCHUFA-Datenbestand abgeglichen. Hierzu werden Name, Vorname, Anschrift, Geburtsdatum, Bankverbindung sowie ggf. eine Voradresse geprüft.

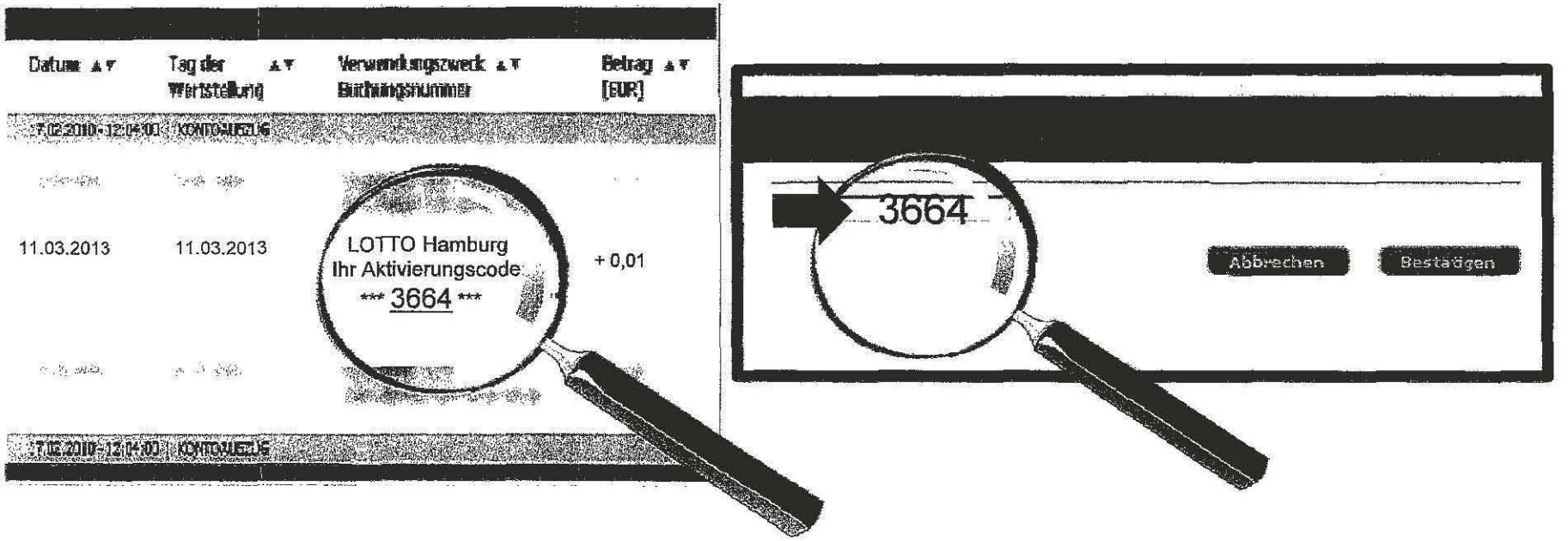
LOTTO HAMBURG

3. Teilprozess: 1-Cent-Überweisung mit Angabe eines Aktivierungscodes

1. 1-Cent-Überweisung mit Angabe des Aktivierungscodes

2. Abschluss der Registrierung durch Eingabe des Aktivierungscodes für Abschluss der Registrierung und zur Freischaltung für LOTTO

Musterbank



Alternativprozess: LOTTO-IDENT-VERFAHREN

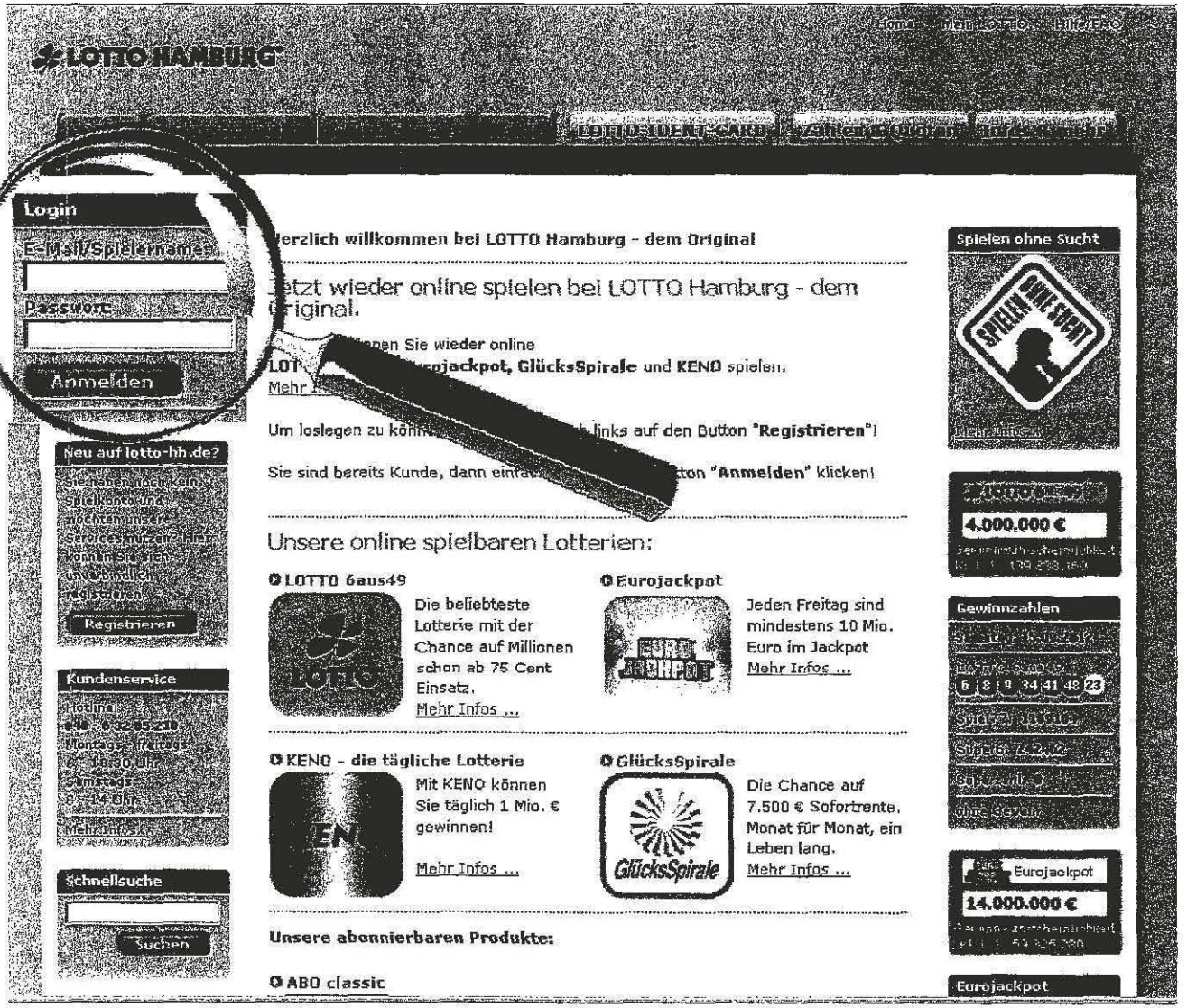
Sofern die oben beschriebenen Teilschritte „SCHUFA JugendschutzCheck“ oder „SCHUFA-KontonummernCheck“ zu keiner positiven Feststellung der zu überprüfenden Daten führen, wird die online-Registrierung abgebrochen.

Alternativ kann der Kunde dann seine Identität und seine Volljährigkeit Face-to-Face in jeder LOTTO-Annahmestelle überprüfen lassen (LOTTO-IDENT-VERFAHREN). Hierzu werden die erfassten Angaben gegen einen amtlichen Lichtbildausweis des Kunden durch das LOTTO-Annahmestellenpersonal abgeglichen.

Dieses Verfahren wurde von der Kommission für Jugendmedienschutz bereits in der Vergangenheit positiv bewertet (KJM-Entscheidung vom Juli 2007 zu Nordwest Lotto und Toto Hamburg).

Authentifizierung (1)

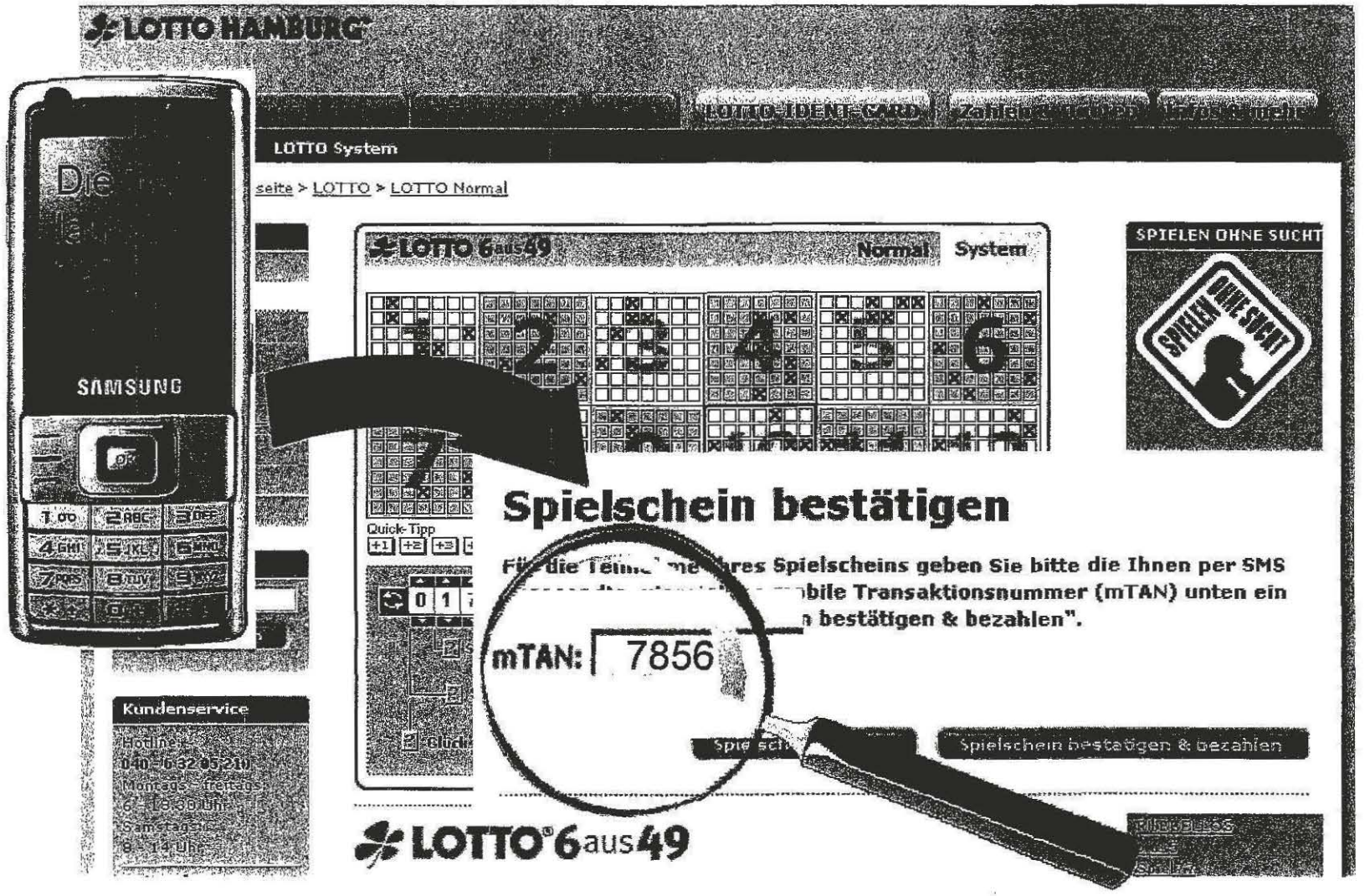
Login durch Eingabe Nutzername/Passwort



Authentifizierung (2)

LOTTO HAMBURG

Spielvertragsabschluss durch mTAN-Eingabe



Freie und Hansestadt Hamburg
Behörde für Inneres und Sport

Behörde für Inneres und Sport, Johanniswall 4, 20095 Hamburg

[redacted]

Bereich Programm und Medienkompetenz
Medienanstalt Hamburg /Schleswig-Holstein
(MA HSH)
Rathausallee 72-76
22846 Norderstedt

Vorab per E-M[redacted]

Amt für Innere Verwaltung und Planung
A 214
Glücksspielaufsicht
Johanniswall 4
20095 Hamburg
Telefon +49 40 42 8 39-3584
Telefax +49 40 42 8 39-4849
[redacted]

23. Juli 2013

Betreff: Identifizierung volljähriger Spieler mittels Alters-Verifikations-System (AVS) der LOTTO Hamburg GmbH
Bezug: Bewertung des AVS aufgrund des Jugendmedienschutz-Staatsvertrages (JMStV) und der Kriterien der KJM hinsichtlich geschlossener Benutzergruppen
Hier: Amtshilfeersuchen zur Bewertung des AVS der LOTTO Hamburg GmbH für ihr Internetangebot

Sehr g[redacted]

die LOTTO Hamburg GmbH hat im März 2013 bei der Medienanstalt Hamburg /Schleswig-Holstein (MA HSH) eine Positivbeurteilung ihres Alters-Verifikations-Systems (AVS) für das Internetangebot www.lotto-hh.de erbeten. Auf ihre Anfrage erhielt die LOTTO Hamburg GmbH am 31. Mai 2013 von der MA HSH die Antwort, dass eine eigenständige Bewertung durch die KJM nur im Wege der Amtshilfe gegenüber der jeweiligen Glücksspielaufsicht erfolgen könne.

Gemäß Artikel I Absatz 1 der „Anordnung zum Erlass sowie zur Aufhebung von Anordnungen über Zuständigkeiten auf dem Gebiet des Glücksspiel- und Spielbankwesens sowie zur Änderung der Anordnung zur Durchführung des Bürgerlichen Gesetzbuches und des Hamburgischen Ausführungsgesetz zum Bürgerlichen Gesetzbuch" vom 18.12.2007 (S. 3252 des Amtl. Anzeigers Nr. 103 vom 28.12.2007) ist die Behörde für Inneres und Sport in der Freien und Hansestadt Hamburg als Glücksspielaufsicht die zuständige Stelle im Sinne des Ersten Glücksspieländerungsstaatsvertrages (GlüStV) und des Hamburgischen Gesetzes zur Ausführung des Ersten Glücksspieländerungsstaatsvertrages (HmbGlüStVAG). Sie überwacht gemäß § 2 Abs. 2 Satz 1 HmbGlüStVAG die Erfüllung der durch den Glücksspielstaatsvertrag oder auf Grund des Glücksspielstaatsvertrages begründeten öffentlich-rechtlichen Verpflichtungen.

Die Behörde für Inneres und Sport, Amt für Innere Verwaltung und Planung, Glücksspielaufsicht (Behörde für Inneres und Sport, Glücksspielaufsicht) bittet daher die MA HSH in o.g. Angelegenheit im Wege der Amtshilfe um eine Bewertung des AVS der LOTTO Hamburg GmbH aufgrund des Jugendmedienschutz-Staatsvertrages (JMStV) und der Kriterien der KJM hinsichtlich geschlossener Benutzergruppen dahingehend, ob das AVS den Anforderungen der KJM für die Altersverifikation und Identifikation von Spielern genügt.

Für Rückfragen stehen wir Ihnen selbstverständlich gerne zur Verfügung.

Mit freundlichen Grüßen

[redacted]

[redacted]

Posteingang
KJM
30. Juli 2013

MA HSH
Medienanstalt Hamburg Schleswig-Holstein

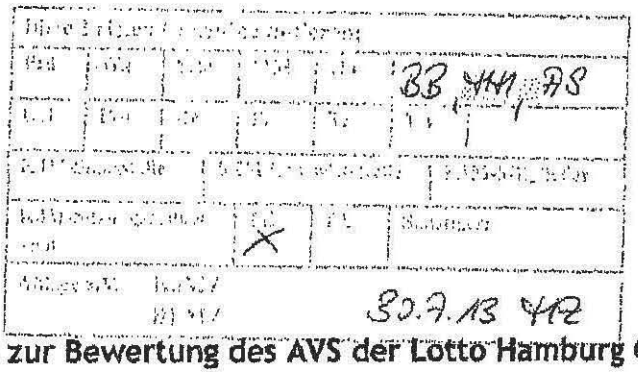
MA HSH · Rathausallee 72 · 76 · 22846 Norderstedt

Kommission für Jugendmedienschutz (KJM)
[redacted]
Heinrich-Lübke-Straße 27
81737 München

Anstalt
des öffentlichen Rechts

Rathausallee 72 - 76
22846 Norderstedt
Telefon 040 / 36 90 05-0
Telefax 040 / 36 90 05-55

E-Mail info@ma-hsh.de
www.ma-hsh.de



AZ 6.5.3.13.1.5
AmtshilfeErsuch an StSt
29. Juli 2013

Amtshilfeersuchen zur Bewertung des AVS der Lotto Hamburg GmbH

Sehr g[redacted],

beigefügt übersende ich Ihnen ein Amtshilfeersuchen der für die Glücksspielaufsicht zuständigen Hamburger Behörde zu dem von Lotto Hamburg entwickelten AV-System.

Die MA HSH übersendet das Amtshilfeersuchen an die KJM mit der Bitte um zeitnahe Prüfung und Votierung.

Die Glücksspielaufsicht Hamburg wurde von uns über den Eingang und die Weiterleitung an die KJM informiert.

Für Rückfragen stehe ich gern zur Verfügung.

Mit freundlichen Grüßen

[redacted]

Anlagen

[redacted]

sie sprachen in unserem Telefonat zwei Punkte zu unserem neuen AVS an, die ggf. noch erhellt werden müssten.

a) **Zeitliche Gültigkeit der PIN**

Die per SMS zugestellte PIN ist für max. 10minuten gültig, danach verfällt sie.

b) **Änderung von Handy-Nummern**

Wie in unserem Konzept dargestellt, zählt die Angabe der Handy-Nummer zu den Stammdaten.

Stammdaten können nur im persönlichen Bereich und nur mit Angabe der zugesandten SMS geändert werden.

Die SMS wird bei Änderung der Handy-Nummer auf die bis dahin gültige/registrierte Handy-Nummer gesimst.

Erst nach erfolgreicher Bestätigung mit der auf die alte Handy-Nummer gesimsten PIN danach kann die

neue Handy-Nummer in Stammdaten eingetragen werden

(die alte Handy-Nummer kann dann nicht mehr genutzt werden).

Mit freundlichen Grüßen

[redacted]

LOTTO Hamburg

[redacted]

Sitz der Gesellschaft: Hamburg
Handelsregister: Hamburg HRB 16709
Geschäftsführer: Michael Heinrich, Torsten Meinberg
Vorsitzender des Aufsichtsrates: Dr. Andreas Reuß

Kommission für Jugendmedienschutz
Der Vorsitzende

11.09.2012

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

(„AVS-RASTER")

(Stand vom 11.09.2012)

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 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

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

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.

Kommission für Jugendmedienschutz
Der Vorsitzende

11.09.2012

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 wiederholten 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://shvv.juris.de/shvv/vvsh-2161.3-0001.htm oder http://www.blja.bayern.de/imperia/md/content/blvf/bayerlandesjugendamt/jugendschutz/vollzugshinweise_zum_jugendschutzgesetz_stand_15.02.2012_11.05.pdf

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:

Identifizierung und Überprüfung von Altersangaben:

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 **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.

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. Post-schalter, 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,[3] durch rechtzeitigen und sicheren Abgleich der Kontenverbindung z.B. mit dem Namen des Kontoinhabers, Alter aller Verfügungsberechtigten etc.).

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

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:

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.