Commission for the Protection of Minors in the Media (KJM)
The Chairman

Criteria for evaluating concepts for age verification systems as elements for ensuring closed user groups in telemedia in accordance with § 4 para. 2 sentence 2 Interstate Treaty on the Protection of Human Dignity and Minors in Broadcasting and Telemedia (JMStV)

("AVS-MATRIX")

(valid since 12.05.2022)

Preliminary remarks*:*

The KJM herewith presents the latest **criteria for evaluating concepts for age verification systems (AV systems or AVS) as elements for ensuring closed user groups in telemedia**, as set out in the statutory provisions of the Interstate Treaty on the Protection of Human Dignity and Minors in Broadcasting and Telemedia (JMStV) - § 4 para. 2 sentence 2. Pursuant to the youth protection guidelines of the state media authorities[1], two interconnected steps must be taken to ensure age verification for closed user groups: the first involves at least one-time identification (age of majority verification), which must be carried out through personal contact. The second is authentication during the individual user process so as to effectively reduce the risk of access authorizations potentially being passed on to minors. There is a difference to be made here between a plausible age verification for the one-time user process (keyword: one-time key) and a reliable age verification for the repeated user process (keyword: master key). Access to the closed user group in both cases may in principle only be activated once the respective procedure has been successfully completed. It is not possible to activate access in advance (so-called "trial access").

The JMStV provides no recognition procedure for closed user groups or AV systems. This is why the KJM has developed a procedure for positive evaluation and evaluates corresponding concepts at the request of companies or providers, where necessary accompanied by discussions or on-site audits. This serves to improve the protection of minors on the internet and is simultaneously a service for providers for more legal and planning security. The main responsibility for the JMStV-compliant configuration of an internet service lies with the content provider, not with the KJM. The content provider must ensure that pornographic content and certain other content deemed harmful to minors can only be accessed by adults (closed user groups) pursuant to § 4 para. 2 sentence

[1] prepared by the KJM, dated 08./09.03.2005; entered into force on 02.06.2005

2 JMStV. This means that they can make use of technical youth protection concepts that have already been positively evaluated by the KJM.

This does not, however, affect additional security obligations, **such as backdoor protection, time limitation of a session, time-out following a certain idle time,** etc., which can be checked in KJM review procedures. This is without prejudice to the fact that the content provider is obliged to ensure that there **is no absolutely inadmissible content in accordance with § 4 Para. 1 JMStV** made accessible in the closed user group.

Possible items for positive evaluations by the KJM:
The KJM evaluates concepts for complete solutions as well as partial solutions (modules) for closed user groups. Modules are evaluated to make it easier for providers to implement them in practice. This gives providers the option of combining positively evaluated modules using a modular principle to create complete solutions for closed user groups, ensuring compliance with the requirements of the JMStV and the KJM. For instance, modules can only be procedures for identifying or authenticating or other essential components of an AV system. Ultimately, however, an AV system is also only a module for a closed user group (even if it is the core component), since it only fulfils the function of "front entry control" for the closed area, but further security measures, such as backdoor protection etc. (see above), must be observed for ensuring a closed user group.
Should a concept, depending on its configuration, be deployable as an AVS within the meaning of § 4 para. 2 sentence 2 JMStV or as a technical means within the meaning of § 5 para. 3 no. 1 JMStV, an evaluation as an "overarching youth protection concept" is possible.

The KJM **has only evaluated concepts to date**. The implementation of closed user groups in practice plays a decisive role in the regulatory assessment.

This **evaluation matrix** for concepts for closed user groups is designed to ensure transparency in the KJM's decision-making processes during evaluation and to define standards. The matrix reflects the current state of the art. However, it is not definitive and leaves room for adaptation and further refinement of the criteria at any time.

I. Concepts of plausible age verification for the one-time user process (keyword: "one-time key")

The use of age confirmation via the eID function of the new ID card, for example, could be conceivable as an age check that is performed again immediately before each use or each access to a closed user group ("one-time key").

Procedures that are suitable for ascertaining the user's age of majority with a high degree of probability (plausibility check) may also be sufficient - similar to the visual check in a video store. A plausibility check is sufficient here since the entire procedure - as opposed to concepts of reliable age verification for repeated user processes (see point II. below) - must be run through for each use.

One way of achieving this is by using a procedure whereby the user is viewed via webcam, to the extent that only trained personnel are used, effective live detection is carried out and sufficient image quality is guaranteed. Live detection and sufficient image quality are required with the aim of ensuring that it is a real person currently sitting in front of the camera and to rule out the potential for circumvention, for instance by using recorded films or masking. If the user is not clearly of legal age, an ID check must also be carried out. Doubts are cast on the basis of the practice during checks in accordance with the German Youth Protection Act, as stipulated by the ministries responsible in the individual federal states in the form of decrees or enforcement instructions[2], if the user's outward appearance, behaviour or statements convey the impression that they could be a minor. If this ID check is conducted via webcam, these requirements also apply here. Care must also be taken to ensure that the ID is inspected from all sides and in full. Access may not be granted if it cannot be established beyond doubt that the user is of legal age.

Simply checking identity card numbers ("Perso-Check procedure") or presenting a copy of an identity card is not sufficient. A certified copy of an ID card will also not suffice, since this only confirms that a document matches, instead of identifying a person.

II. Concepts of reliable age verification for the repeated user process (keyword: "master key")

The reliable age verification for the repeated user process involves two steps: one-time identification and authentication of the identified person for each user process. Once they have

[2] See e.g. http://shvv.juris.de/shvv/vvsh-2161.3-0001.htm or http://www.blja.bayern.de/imperia/md/content/blvf/bayerlandesjugendamt/jugendschutz/vollzugshinweise_zum_jugendschutzgesetz_stand_15.02.2012_11.05.pdf

been identified one time, users who are recognised as being of legal age and consequently authorised are issued with a kind of "master key" for all follow-up user processes. This entitles them to access any number of different services. When compared to the one-time key mentioned above or when compared to a retail store with offers for adults (e.g. video store), in which only a limited number of products are usually purchased or borrowed, the requirements are correspondingly higher. Checking the age of the person simply by looking at them does not meet the requirements here.

A. Identification

It is only possible to ensure a closed user group for adults by means of a reliable age check or age of majority check. The **face-to-face** identification of natural persons, including verifying their age, is a prerequisite to ensure reliable age verification. It is necessary to identify individuals personally in order to avoid the risk of forgery and circumvention to the greatest extent possible.

The requirements of the KJM are specified as follows:

Verifying and identifying age information:

1.) Face-to-face identification:

Face-to-face contact must always be used to identify interested parties for a closed user group at least once. "Face-to-face contact" is generally understood to mean a check between persons present ("face-to-face" check) involving a comparison of official identification data (identity card, passport).

Such is the case, for example, with procedures such as "Post-Ident" or comparable procedures.

It may also be possible, subject to certain conditions (see below), to refer back to a "face-to-face" check that has already taken place. Such is the case, for example, when using identification procedures by means of verified personal and age or birth data that have already been recorded when taking part in certain services or concluding certain contracts (e.g. mobile phone contracts, opening bank accounts in compliance with the German Money Laundering Act; participation in the DE-Mail communication service; use of the eID function of the new ID card) by comparing it with official ID card data.

Simply checking identity card numbers ("Perso-Check procedure") or presenting or sending a **copy of an identity card** is not sufficient. A **certified copy of an ID card will also not suffice**, since this only confirms that a document matches, instead of identifying a person

Identification via webcams alone **does not** constitute sufficient reliability as an initial age check for repeated use and consequently does not comply with the requirements for reliable identification within the meaning of the KJM benchmark criteria.
Where additional security measures are in place (see circular letter 03/2017 (GW) - Video identification procedure of the Federal Financial Supervisory Authority[3]), this may, however, satisfy the requirements for reliable identification within the meaning of the KJM benchmark criteria.

There is no need for a face-to-face check if identification is performed using software by comparing the biometric data on the ID document with a photograph of the person to be identified and automatically recording the data on the ID document.

There is no need for a face-to-face check by comparing official ID data (ID card, passport) if the age check uses a procedure based on automated camera-based age determination, in the context of which software draws conclusions about the probability of the age of the person to be identified on the basis of biometric features of a live camera image and in doing so, achieves the level of reliability of a personal age check.[4]

2.) Recording and storage of the data required for identification:

The personal data of the person to be identified that is required for the age check should be recorded and stored to the required extent in compliance with data protection regulations (e.g. date of birth, name, address). It is only sufficient to record only the age of the identified person when this is linked to unique authentication features in the same step.

[3] retrievable at https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html

[4] BGH judgement dated 18.10.2007 – I ZR 102/05 - ueber18.de; the reliability of the age estimation in the relevant age groups 13 to 18 must be ≥ 95% in this case.

3.) Requirements for data collection points:

The identification data can be recorded **at a number of different locations** (e.g. post-office counters, a range of sales outlets such as mobile phone provider shops, lottery retailers, banks and savings institutions, etc.). A **complete recording** of the **personal data** relevant to the age check in an offline or online form and its **forwarding to the AVS operator** must be ensured. It is also sufficient to transfer a reference pointer to the recorded data (storage location, specific source) to the AVS operator as an alternative to forwarding the data. The data collection point's suitability within the meaning of the JMStV is contingent upon it being **run on a commercial basis by reliable staff with sufficient training in the task at hand.**

4.) Final age check:

It is only possible to access the closed user group (activation of user data for authentication) once the **AVS operator has received the identification data or a reference pointer to it and has checked the age**. The AVS operator can only use the initial identification data to check whether the user is an authorised adult user each time they enter the closed user group (authentication).

<u>Transfer of access keys to the user:</u>

If access keys (e.g. activation codes, hardware components or the like) are not already handed over to the user personally during the registration process or generated within the context of the registration, but instead need to be delivered or otherwise transmitted afterwards, care must be taken to ensure that the access keys are only passed on to the person identified as being of legal age.

In the case that a "face-to-face" check has already been performed (see above), an access key must be delivered by registered mail by hand or a method of similar qualification. A variant is deemed to be similarly qualified provided it ensures that only the person identified as being of legal age receives the access data. The reason behind this is that an identity that is initially only asserted must be verified against an actual identity (see above). An anonymous handover or delivery of access authorisations, e.g. by means of a simple e-mail or account statements, is therefore not sufficient. It must rather be assumed with sufficient certainty that only the person previously identified as being of legal age gains access to the information transmitted in this manner (e.g. delivery by DE-Mail subject to certain conditions,[5] through timely and secure cross-checking of the account details, e.g. with the name of the account holder, age of all parties authorised, etc.).

B. Authentication

Authentication is used to ensure that only the respectively identified and age-approved person has access to closed user groups and is intended to impede the transfer of access authorisations to unauthorised third parties. The following must be ensured in this case:

<u>Granting access to users:</u>

- **Performing authentication at the start of each user process ("session").**

- **Safeguarding content within the meaning of § 4 para. 2 JMStV through a special, individually assigned password** (not necessary for biometric procedures, since the authorised person is identified beyond doubt)

<u>Prevention of transfer/multiplication:</u>

Sufficient protective measures must be put in place to prevent the multiplication and use of access authorisations by unauthorised third parties. Transfer protection can be realised <u>either</u> through technical measures to impede multiplication (see solution variant 1: hardware solution/unique identifier solution) <u>or</u> through personal risks in the user's sphere (see solution variant 2: risk solution).

- **Solution variant 1: possible technical measures for impeding the multiplication of access authorisations ⇒ HARDWARE or UNIQUE IDENTIFIER SOLUTION:**

- **Verification of biometric data:** access to the closed user group is only granted to users who have prior identification and who are able to authenticate themselves using biometric data (e.g. fingerprint, iris recognition). Access authorisations cannot be

[5] See in more detail below on the level of authentication

multiplied or used by third parties, providing sufficiently secure verification components are used when capturing biometric data and authentication.

- **Active hardware component:** active hardware (e.g. ID chip, SIM card) has the capability of performing computing operations on the chip. This means that it can only be reproduced with great effort. Access authorisation (hardware + password) can consequently only be passed on to a single person sequentially.

- **Passive hardware component:** unlike active hardware, passive hardware solutions (e.g. passive chip cards, also DVD, CD-ROM) are only capable of storing data and are not technically equipped with their own CPU. These components can, however, under certain circumstances be read out and duplicated or the communication of the end device with the hardware can be emulated. This is why these components must not be capable of being copied trivially and - to the extent that they can be read out - it must not be possible to use the read-out data for purposes other than those for which it was intended.

- **One-time PIN procedure (e.g. using a token generator or one-time PIN via SMS to the registered SIM card):** PIN-TAN lists cannot guarantee sufficient protection against multiplication, since multiple accesses are available here in principle. By contrast, one-time PIN procedures, whereby copy-protected hardware is used for generating or obtaining access authorisations that can only be used once, are sufficient.

- **Identification of the end device:** this is where the computer itself or the respective output device is used for protection against multiplication and forwarding of access authorisations (e.g. querying the processor ID). It can be ensured with sufficient security that an access authorisation can only be used on a single end device by means of a corresponding combination of access software and hardware of the end device.

- **Solution variant 2: subjective impediment of unauthorised use of access authorisations within the sphere of the user (reduction in the risk of passing on) ⇒ RISK SOLUTION:**

  The risk of an authorised user disclosing their access authorisations to unauthorised third parties can be reduced to the extent that they may incur considerable material or immaterial disadvantages. The user must be clearly informed of this as part of the registration process. In this regard, the presumed "tangibility" of the disadvantages in the

individual case must determine whether a disclosure risk is sufficient. It is insufficient if these are only manifested in areas of life that are purely virtual.
Considerable disadvantages within the meaning of the above are to be assumed, for instance, if the disclosure of data poses a permanent risk of high costs being incurred and/or important secrets being revealed:

- **Cost risk:** there is a high financial risk, for example, if the authorised user's current account or credit card can be charged in a relevant amount and on an ongoing basis when using the access authorisation. Prepaid procedures without any further financial risk are not sufficient in this respect.

- **Secret risk:** a high risk in relation to the exposure of secrets is given, for example, when an unauthorised third party is able to gain insight into relevant (highly) personal life areas of the user when the access authorisation is used and may also be able to modify such information on their own authority, e.g. health data, payment transaction information, etc.

The ideal situation is that such risks are combined. Otherwise, access must be cancelled immediately with regard to the cost risk if the user's account is not credited.