Federal Agency
for Child and Youth
Protection in the Media

Criteria for examining the suitability and effectiveness of precautionary measures taken by providers of digital services pursuant to section 24a of the Youth Protection Act

Examination criteria of the Federal Agency for Child and Youth Protection in the Media

According to sections 24 *et seq.* of the German Youth Protection Act (*Jugendschutzgesetz – JuSchG*), providers of digital services storing or providing third-party information for users on a for-profit basis shall ensure via suitable, effective structural precautionary measures that the protection goals of section 10a numbers 1 to 3 of the JuschG are complied with:

1. protection against media detrimental to development,
2. protection against media harmful to minors,
3. protection of the personal integrity of minors when using media.

The Federal Agency for Child and Youth Protection in the Media (*Bundeszentrale für Kinder- und Jugendmedienschutz – BzKJ*) is responsible for the supervision of the structural precautionary measures to be taken by the providers of digital services and examines their implementation, concrete form and suitability. In the context of this multi-stage process under section 24b of the JuSchG, the BzKJ is also authorised to order specific precautionary measures to be taken and, in case of non-compliance, impose fines of up to 50 million euros.

The following examination criteria of the BzKJ shall offer guidance to providers of digital services regarding the risks to be mitigated by means of suitable structural precautionary measures. Additional details are provided on the criteria used by the BzKJ to assess the suitability and effectiveness of precautionary measures taken by providers of digital services. Furthermore, this overview offers other parties responsible for child and youth media protection as well as the general public an insight into the internal processes of the BzKJ.

I. Risk assessment

Suitable and effective structural precautionary measures are based on a valid assessment of the actual risks associated with the concrete use of a specific digital service by children and juveniles. The Gefährdungsatlas (Risk Atlas), which is published by the BzKJ, contains a scientific and detailed presentation of media phenomena and their associated risks that serves as a comprehensive technical basis for the risk assessment.

These risks can be divided into three categories:

1. **Exposure to content that is detrimental to development and harmful to minors (exposure risks)**

   Examples: extremist content, age-inappropriate sexual content, violence, disinformation and conspiracy narratives, advertisement and distribution of substances harmful to health, pro-ana/pro-mia as well as other pro-ED content, suicide forums, presentation of children and juveniles as sex objects.

2. **Interaction with harmful third parties (interaction risks)**

   Examples: cybergrooming, cyberbullying, cyberstalking, abusive distribution of intimate content, fake accounts intended to cause harm, identity theft, digital pillory/doxing.

3. **Risks relating to a service's specific design and the individual's use pattern (usage risks)**

   Examples: cost traps, (simulated) online gambling, internet addiction and excessive media use, algorithm-based recommendation systems, referral loops, a lack of transparency regarding or misuse of personal data, creation and analysis of user profiles, excessive self-promotion, unintelligible Terms and Conditions.

II. Risk mitigation

According to section 24a JuSchG, providers must take effective and suitable structural precautionary measures to mitigate the three risk categories mentioned above. Depending on the specific risks associated with a given service, above all, the following structural precautionary measures are to be implemented:

- Reporting and remedy procedures (section 24a (2) No. 1 and No. 2 of the JuSchG),
- Age-based rating system for user-generated audiovisual content (section 24a (2) No. 3 of the JuSchG),
- Age verification (section 24a (2) No. 4 of the JuSchG),
- References to offers of advice, assistance and reporting independently of providers of digital services (section 24a (2) No. 5 of the JuSchG),
- So-called parent support tool (*Elternbegleitungstool*) that allows persons having custody to guide children's media use (section 24a (2) No. 6 of the JuSchG),
- Secure default settings limiting usage risks (section 24a (2) No. 7 of the JuSchG),
- Child-appropriate Terms and Conditions (section 24a (2) No. 8 of the JuSchG).

As suitable instruments of risk mitigation, the structural precautionary measures listed in the JuSchG can generally be ascribed to the three risk categories as follows :

Risk assessment ↓	Risk mitigation ↓
Risk categories	**Structural precautionary measures**
1. Exposure risks → Exposure to content that is detrimental to development and harmful to minors Examples: extremist content, age-inappropriate sexual content, violence, disinformation and conspiracy narratives, advertisement and distribution of substances harmful to health, pro-ana/pro-mia as well as other pro-ED content, suicide forums, presentation of children and juveniles as sex objects.	**Preventive measures** ➢ Reporting and remedy procedures for content that is detrimental to development/harmful to minors ➢ Age-based rating system for user-generated content – specifically regarding media content for users over 18 ➢ Age verification
2. Interaction risks → Interaction with harmful third parties Examples: cybergrooming, cyberbullying, cyberstalking, abusive distribution of intimate content, fake accounts intended to cause harm, identity theft, digital pillory/doxing.	**Precautionary measures** ➢ Reporting and remedy procedures for risks to personal integrity ➢ References to offers of advice, assistance and reporting independently of providers of digital services ➢ Secure default settings, particularly regarding age groups, anonymity, undisclosed location, restriction of communication and contacting options
3. Usage risks → Risks relating to a service's specific design and the individual's use pattern Examples: cost traps, (simulated) online gambling, internet addiction and excessive media use, algorithm-based recommendation systems, referral loops, a lack of transparency regarding or misuse of personal data, creation and analysis of user profiles, excessive self-promotion, unintelligible Terms and Conditions.	**Precautionary measures** ➢ Parent support tool that seeks to modify the patterns of use of minors by offering control and support systems for persons having custody, especially with regard to time limits and purchase options (known as Elternbegleitungstool) ➢ Information on specific risks/guidance ➢ Child-appropriate Terms and Conditions

Figure 1: Structural precautionary measures taken by providers of digital services as instruments of risk mitigation
Source: Federal Agency for Child and Youth Protection in the Media (BzKJ)

Requirements for the various precautionary measures

To ensure children and juveniles can partake in digital services as safely and untroubled as possible, the BzKJ always verifies the compliance of the providers of digital services obligated under section 24a (1) JuSchG with the requirements for the various precautionary measures listed below in connection with the respective risks.

These requirements explicitly do not preclude providers of digital services from taking additional measures, which can be included and taken into account in the overall assessment of the effectiveness and suitability of the prevention and/or, in individual cases, lead to exceptions from the assessment benchmarks. Additional measures may, for instance, be required if they are deemed necessary due to the design and inherent risks of a digital service. The aim is to ensure a suitable and effective prevention in line with the individual risks associated with the use of the digital service in question.

The following requirements for the individual precautionary measures are regularly examined:

1. Reporting system

- The reporting option must be easy to find and permanently available when perceiving the content.
- The reporting option must be accessible in no more than two clicks via a clearly labelled link.
- The reporting system must be easy to use and understand for average minor users, especially with respect to the user interface. It is generally not considered easy-to-understand if, for instance, sending a report requires legal knowledge, such as when the only reporting option available is labelled “Reporting under the Network Enforcement Act” or when other reporting categories are used that are obviously unclear or confusing to children and juveniles, including designations that are overloaded with technical terms.
- The reporting option must also be available to non-registered users if the content is accessible to them.
- There must be an option for giving individual reasons for one’s complaint/report, but the person reporting must not be required to provide such justification.

2. Reporting-based remedy system of the service provider

- The reported content must be checked without delay. The users’ assessment does not limit the providers’ of digital services obligation to examine complaints.
- If the examination of this reported content confirms that the complaint was justified, the content in question shall be removed or access to it denied without delay.
- After the examination of the report, the person who submitted the report shall be informed about the outcome of the examination as well as further options.
- Information shall also be provided about the arbitration procedure in accordance with the Interstate Treaty on the Protection of Minors (*Jugendmedienschutz-Staatsvertrag*), which is regulated by Land law.

3. Options to seek legal redress after the service provider’s decision in the context of the reporting procedure

- Both parties to the procedure (the person reporting and the person being reported) have the option of remonstration, i. e., both parties can file an objection and remonstrate against decisions that are unfavourable to them.

- The remedy procedure ensures that the person submitting the report is advised right from the beginning and in an appropriate manner about the fact that the content of their report can be passed on to the users concerned, without, however, allowing the information to be traced back to the person having submitted the report.
- The platform provider must review its first decision immediately should it receive a remonstrance from the other party. The platform provider must justify its decision without delay, referring specifically to the individual case in question.

4. Age-based rating system for user-generated audiovisual content

- The platform provider offers a rating system with which users are requested to evaluate whether user-generated audiovisual content is suitable only for users aged 18 years or over.
- There must be a possibility for other users to report incorrect ratings performed with or without malicious intent quickly and without significant effort (reporting and follow-up control mechanisms).

5. Age verification

- As soon as a provider of digital services content labelled as "over 18" (see number 4), it must regulate access to this content by means of a recognised age verification system. A system is considered as recognised, for instance, if it is rated as positive by the Commission for the Protection of Minors in the Media (*Kommission für Jugendmedienschutz – KJM*)

6. References to offers of advice, assistance and reporting independently of providers of digital services

- Depending on the services offered, the platform provider must give individually tailored, easily found suggestions on where to find offers of advice, assistance and reporting that are not associated with the providers of digital services. For instance, a reference to specialised counselling agencies may be needed if there is evidence of risks with respect to sexual violence against minors, self-harm, suicide, hate speech or extremism. One example for an external suicide prevention service is the "*Telefonseelsorge*" helpline.
- The external counselling services referred to should not be restricted to telephone helplines, but should include diverse, youth-friendly contact options (such as chats). The counselling services must be available in German; additional languages would be desirable.
- If the references to external counselling services are grouped together within a support area, this area must be accessible directly within the service and not only after being redirected to another website. In view of the patterns of use of children and juveniles, a notice appearing, for instance, directly upon submitting a report or being exposed to specific content, is to be preferred.

7. Parent support tool that allows persons having custody to guide children's media use

- This tool (known as *Elternbegleitungstool*) must be easy to find and user-friendly, suited to addressing the service's specific risks and contain the following functionalities, depending on the service:
    - a timing feature (displaying the time the child or youth has spent on a platform),
    - a feature for setting a limit to the amount of money that can be spent over a specified period of time and/or the general option to require parental consent for any financial expenditure,

  - additional, case-specific features to guide and monitor internet use by minors with regard to content that may be detrimental to their physical, mental or moral development.
- The following applies with regard to design:
  - The respective settings must be easy to find.
  - The monitoring options must be described in a clear and easy-to-understand manner, underpinned, if necessary, by help and support areas.
  - The activated settings must apply independently of the device used so that, for instance, it does not make any difference which operating system is used.
  - The settings cannot be changed without authorisation from the person having custody and must remain in place even after software updates.
  - The child or youth's privacy is not unduly restricted by the parental guidance. For instance, persons having custody may not be able to read the child's or youth's personal messages.

8. Secure default settings limiting usage risks

- Providers of digital services must offer secure default settings to protect minor users against usage risks and activate those settings at registration. This includes, in particular, that
  - user profiles of children and juveniles cannot be found by search engines,
  - user profiles of children and juveniles cannot be viewed by people that are not logged in,
  - the location, contact details and communications of minor users are not published,
  - the visibility of user profiles of minors is limited to the group of people they have selected themselves and unwanted contact requests from strangers are prevented,
  - an option exists for service usage that makes it near impossible to identify the actual minor users, e. g. by pseudonymisation.

9. Child-appropriate Terms and Conditions

- The provisions in the Terms and Conditions essential to use must be tailored to the specific services offered and provided in a child-appropriate manner, i. e. they must be phrased, adapted and presented in an age-appropriate manner.
- How this obligation is implemented is the sole responsibility of the providers of digital services. The BzKJ does not verify the Terms and Conditions in terms of content, but only assesses whether the material provisions of the Terms and Conditions have been adapted in a way that is easy to understand for children and juveniles.

Notes

The above-mentioned requirements for structural precautionary measures according to the Youth Protection Act do not preclude that further legal requirements to the service may become necessary for other reasons such as regarding data protection law.

The examination criteria are regularly assessed and revised, especially in the context of the BzKJ's ZUKUNFTSWERKSTATT[1] (FUTURE WORKSHOP) discussion format, with regard to changing requirements in the services landscape as well as on the basis of the steadily growing body of science or new insights from the advisory council of the BzKJ. These criteria are therefore subject to change.

Contact

Federal Agency for Child and Youth Protection in the Media
Rochusstraße 8-10
53123 Bonn

E-Mail: info@bzkj.bund.de
Internet: www.bzkj.de

[1] In the context of the BzKJ's ZUKUNFTSWERKSTATT (FUTURE WORKSHOP) dialogue format, providers of digital services as well as interdisciplinary experts and representatives from the fields of child and youth protection and youth work meet up to talk about smart options for managing the risks and opportunities regarding the implementation of childrens' rights in the digital space. This includes, in particular, discussions on precautionary measures taken by providers of digital services.