Safety by design requirement: requirement to implement preemptive protection measures

Summary

Law	Sec. 24a Youth Protection Act				**Effective date:**		1 May 2021				
Applies to:	Social networks	Search Engines	Game distribution platforms	VoD platforms	App stores	Video games	Movies and shows	Video-sharing platforms	Media compilation apps and services	Smart devices/ connected devices	Messenger services
	Yes		Depends			Depends		Yes			Yes

Content of the regulation — quick overview

- Services that store or provide third-party information for/to other users have to implement preemptive protection measures.
- Exemptions apply, among others, to services with fewer than 1m users in Germany.
- The question of which measures have to be implemented is subject to a flexible standard and a case-by-case decision, factoring in all risks deriving from the service.
- Fines up to EUR 50m are possible in the worst case.

Applies to abroad companies?	Yes
EU/EEA country of origin principle respected?	Yes

Contents

I. Who is affected by the regulation?

II. What are the requirements?

III. Enactment

IV. Sanctions

V. Risk mitigation and compliance procedures

I. Who is affected by the regulation?

In-scope services:

According to Sec 24a (1) of the Youth **Protection** Act, **service providers that store or provide third-party information for/to other users** for profit must take appropriate and effective structural precautions to ensure that the protection objectives of the law are met (preemptive measures).

The obligation applies to:

- classic **host providers** such as **social networks, discussion boards and video-sharing platforms**
- **online games** as per the legislator's explicit comments in the explanatory section of the law, but only to the extent that the game includes content-sharing and/or in-game chat and messaging features or similar functions (though the requirements in this regard are low)
- **distribution platforms** that offer social media, messaging, discussion and video-sharing features
- **messenger services** are most likely also caught to the extent that they do not qualify as telecommunication services

Exemptions:

- nonprofit services
- services not directed at minors and that are typically not used by them (e.g., professional networks)
- services that provide editorial content that is provided by the service provider itself
- platforms that can demonstrate that they have less than 1 million users in Germany

Companies outside of Germany:

- The requirement, including the possibility to impose fines for violations, explicitly applies to game distribution and VoD platforms that do not have their seat in Germany.
- EU/EEA country of origin principle:
  - The law respects the EU/EEA country of origin principle.
  - The **country of origin** principle under the Audiovisual Media Services Directive and the E-Commerce Directive applies to service providers established in another EU/EEA member state.
  - Service providers that can rely on the EU/EEA country of origin principle are exempted, as they only have to comply with the youth protection laws in their EU/EEA country of origin.
  - However, the requirements for an actual establishment have to be met (e.g., mere shell companies are not sufficient for this purpose). The exact requirements for an establishment under the Audiovisual Media Services Directive and the E-Commerce Directive country of origin principle, as well as the exemptions from it, differ in detail.
  - The country of origin principle allows for exemptions, in particular, in the area of youth protection. The German youth protection regulator recently started to test these exemptions and it is currently unclear whether this will become an ongoing practice in the future. To **mitigate** this risk, see the relevant risk mitigation procedures section below.

II. What are the requirements?

- The provision establishes a **safety-by-design standard**, which requires services to implement certain preemptive protection measures to ensure that the objectives of the amended Youth Protection Act are met.
- The **protection objectives** are as follows:
  - protection against content that impairs the development of minors or that is harmful to minors (e.g., violent content)
  - protection of personal integrity, in particular, against interactional and communication risks such as the following:
    - communication and contact functionalities (e.g., in-app or in-game voice, text or video chats and messaging features)
    - purchase functionalities (e.g., in-app and in-game purchases)
    - gambling-like mechanisms (e.g., loot boxes or simulated gambling)
    - mechanisms that encourage excessive media use (e.g., games that incentivize coming back to the game through time-dependent rewards or game mechanisms that could be considered to be encouraging excessive playing)

        - sharing user data without consent (e.g., sharing in-game progress/statistics or location data on social networks)
        - purchase exhortations that are not age-appropriate, in particular, advertising for other media (e.g., including trailers or ads for a 16+ game/movie in a 12+ game)

- The question of which preemptive measures have to be implemented **is subject to a flexible standard and a case-by-case decision, factoring in all risks deriving from the relevant service**:
    - The higher the risks (from a Youth Protection Act perspective), the more robust the preemptive measures have to be.
    - This **flexible standard** is similar to the concept of technical and organizational security measures under data protection law, which also requires adequate measures to be implemented for the overall risks.
    - In particular, the more interactional and communication risks (see the list above) that are included in a service, the higher the overall risk of such service from a Youth Protection Act perspective.
    - **Example:** A mobile game that is primarily played by children and that includes in-game chats, in-game purchases, loot boxes and other social network-sharing features will likely have to implement more preemptive measures than a mobile game that only has in-game purchases.
- The Youth Protection Act contains a **catalog of preemptive measures** (see below), which only serve as examples (sec. 24a (2) Youth Protection Act), as follows:
    - Introducing all or most of these exemplary measures grants a de facto assumption that the service provider is compliant with the safety-by-design requirement. The wording "in particular," as included in the law, suggests that the legislator prefers the implementation of the measures proposed by the law.
    - Nevertheless, since the provision establishes a flexible standard and because the catalog explicitly only lists examples, the provider does not have to implement every single one of the suggested measures. Technically, the provider does not have to implement any of the proposed measures if the risks, design and nature of the service makes others measures more appropriate and efficient.
    - The service provider can excel with regard to one of the suggested preemptive measures (e.g., by introducing a particularly robust one) and, therefore, can fall short on another or replace it with an entirely different measure that is as effective but more appropriate considering the specific risks of the service.
    - The following example measures are suggested in the law:
        - providing a **notice and takedown procedure** for content that can impair the development of minors or that is harmful to them (e.g., violent or scary/horror content; this measure is primarily relevant for social media and video-sharing-platforms)
        - providing a **reporting feature** with a user interface for children by which minors can report impairments for their personal development (e.g., a content or in-app, in-game or in-chat reporting function that allows reporting on cyberbullying, defamation, grooming through communication or content, etc.)
        - providing a **self-rating system for user-generated audiovisual content** that allows users to self-rate content as 18+ (primarily relevant for social media and video-sharing platforms; this measure is supposed to partially implement Art. 28b (3) (g) of the Audiovisual Media Services Directive)

- providing **technical means for age verification** for user-generated audiovisual content that was self-rated with 18+ (primarily relevant for social media and video-sharing platforms; this measure is supposed to partially implement Art. 28b (3) (f) of the Audiovisual Media Services Directive)
- easy-to-find **information** on third-party **counseling** and **support** services, as well as third-party **reporting channels** (e.g., support/counseling for victims of cyberbullying or information where criminal behavior can be reported to the authorities)
- providing **technical means for controlling and monitoring the use by parents** (this measure is supposed to partially implement Art. 28b (3) (h) of the Audiovisual Media Services Directive):
  - Examples could be parental control functions that deactivate in-app purchases, deactivate certain in-app ads, deactivate in-app chats and messaging functions, deactivate/restrict loot boxes, limit the play time, set spending limits, prevent the sharing of personal data and other data protection settings, restrict unsuitable content, etc.
  - The German self-control organizations the USK (for games) and the FSM (for all other online services) allow the official certification of parental control functions as a "closed system" (for instance, the Nintendo Switch's parental control functions were certified as a closed system). Such a certification is an attractive solution for distribution platforms in particular, which include social media features. The certification would be a strong argument that the platform is compliant overall with the requirement to implement safety-by-design. The certification process should be prepared well in advance.
- implementing **youth-protection-by-default settings** that restrict the use risks for minors under consideration of their age, as follows:
  - user profiles may by default not be found by search engines or viewed/accessed by other registered users
  - location and contact data, and communication with other users are not published by default
  - default restriction of the communication of the user to a selected group of other users as predefined by the user
  - the use of the service by default takes place only anonymously or under a pseudonym
- general terms and conditions that outline the essential conditions to use the service in a child-friendly manner

- Social networks and video-sharing platforms that already comply with the **German law against hate speech** (the Network Enforcement Act - "NetzDG") only have to implement preemptive measures to the extent that they were not already implemented for the purposes of NetzDG compliance. For instance, the NetzDG requires the implementation of a notice and takedown procedure for certain content as defined in the NetzDG (e.g., Holocaust denial). Services that already comply with the NetzDG requirement to implement a notice and takedown procedure do not have to implement a second notice and takedown procedure. However, they have to amend the existing procedure to allow the notification and takedown of content that falls under the Youth Protection Act (e.g., 16+ or 18+ content such as trailers, violent gameplay videos, horror film scenes, etc.)

III. Enactment

- The amended Youth Protection Act came into force on 1 May 2021.

IV. Sanctions

- Compliance with the obligation to implement preemptive measures will be supervised by the newly implemented Federal Agency for the Protection of Children and Young People Within Media ("**Federal Agency**").
- Jugendschutz.net (a youth protection organization) will conduct reviews of the preemptive measures implemented by different service providers and report the outcome to the Federal Agency.
- If the Federal Agency determines that a service provider has not implemented sufficient measures, it will give the service provider the opportunity to provide a statement and it will discuss the required preemptive measures together with the service provider.
- If the service provider does not implement the measures that are considered adequate by the Federal Agency, the Federal Agency will request that the service provider implement such measures within a reasonable time.
- If the service provider does not implement the required measures within a reasonable time, the Federal Agency can issue an order to implement the measures.
- If the service provider does not comply with the order, the Federal Agency can impose **a fine of up to EUR 50 million**.

V. Risk mitigation and compliance procedures

- The Youth Protection Act includes **two risk mitigation** procedures, as follows:
  - **The first procedure** helps to gain legal certainty in relation to whether the service is compliant with the requirement to implement preemptive measures:
    - The first procedure is recommended for the largest service providers and it can be compared to the concept of Binding Corporate Rules under the General Data Protection Regulation.
    - The procedure requires the execution of a recognition procedure by defining and implementing specific preemptive measures in a self-imposed guideline (Sec. 24b (2) of the Youth Protection Act).
    - In addition, the guideline must be agreed on with one of the recognized self-control organizations (in practice, primarily USK.online for video games and the FSM for all other online services) of which the service provider has to be a member.
    - Next, the Federal Agency has to confirm that the guidelines are adequate.
    - Last, the guideline has to be published by the Federal Agency, the service provider and the self-control organization. The publication process has to meet certain requirements.
  - The **second procedure** helps to gain legal certainty in relation to whether the requirement to implement preemptive measures applies at all to the operated service:
    - Service providers may request that one of the recognized self-control organizations (in practice, primarily USK.online for video games and the FSM for all other online services) determines that the obligation to implement preemptive measures does not apply to them (Sec. 24b (5) of the Youth Protection Act).
    - This procedure is interesting for service providers that
      - take the position that their service does not "store or provide third-party information for/to other users" and would like to have this position confirmed and/or

  - want to rely on the EU/EEA country of origin exemption and would like to obtain (semiofficial) confirmation that the exemptions from the country of origin principle do not apply and/or
  - can prove that their service has less than 1 million users in Germany
- If USK.online or the FSM confirm the position, the regulator (the Federal Agency) can only regulate the service under very limited circumstances, which in practice almost never apply.

- We reiterate the possibility for service providers to obtain a certification as a "closed system" by USK.online or the FSM. This option is particularly recommended for video game distribution platforms that provide interactional and communication features for which they have already implemented parental controls. The certification would be a strong argument that the platform is compliant overall with the requirement to implement safety-by-design.

For further questions don't hesitate to contact our specialists:

Sebastian Schwiddessen LL.M.
Senior Associate
sebastian.schwiddessen@bakermckenzie.com

Andreas Jagusch
Associate
andreas.jagusch@bakermckenzie.com

Baker & McKenzie - Partnerschaft von Rechtsanwälten und Steuerberatern mbB

Berlin
Friedrichstraße 88/Unter den Linden
10117 Berlin
Tel.: +49 30 2 20 02 81 0
Fax: +49 30 2 20 02 81 199

Frankfurt am Main
Bethmannstraße 50-54
60311 Frankfurt am Main
Tel.: +49 69 2 99 08 0
Fax: +49 69 2 99 08 108

Düsseldorf
Neuer Zollhof 2
40221 Düsseldorf
Tel.: +49 211 3 11 16 0
Fax: +49 211 3 11 16 199

München
Theatinerstraße 23
80333 München
Tel.: +49 89 5 52 38 0
Fax: +49 89 5 52 38 199

www.bakermckenzie.com

Get connected: