MMR
Zeitschrift für IT-Recht und Recht der Digitalisierung

in Kooperation mit: Bitkom · davit im DAV · eco · game · Legal Tech Verband · VAUNET

CHRISTIAN-HENNER HENTSCH / KONSTANTIN EWALD / ROLF SCHWARTMANN (Hrsg.)

Digital Services Act and Game

Osborne Clarke

Kölner Forschungsstelle für Medienrecht
Technology Arts Sciences TH Köln

game Verband der deutschen Games-Branche

Supplement to MMR
8/2025

Pages 663–684
28. Jahrgang · 15. August 2025

1851202518

MMR

Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT

In Kooperation mit: Bitkom – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. · davit im DAV – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein · eco – Verband der Internetwirtschaft e.V. · game – Verband der deutschen Games-Branche e.V. · Legal Tech Verband Deutschland e.V. · VAUNET – Verband Privater Medien

Supplement to MMR 8/2025

EDITORIAL

The role of the Digital Services Coordinator

reading time: 7 minutes

In our everyday lives, we are surrounded by services that transmit information, possibly save it and publish it in a way that is visible to third parties. These are classed as intermediary services. They are mostly online platforms and hosting services but also include caching and „mere conduit" services. We use the best known of these services – social media platforms like Instagram, TikTok or X and online marketplaces such as Amazon, Temu and eBay – almost constantly.

The intermediary services that we use can therefore have a great influence on the opinions we form, the decisions we make and our safety. For this reason, the European Commission has adopted various Regulations as part of its Digital Strategy to regulate the impact of these intermediary services.

One of these is the Digital Services Act (DSA), which aims to create a safe, predictable and trusted online environment for recipients of the services, that is to say, the users. It fully entered into force on 17 February 2024, strengthening in particular the rights and options of recipients to take action themselves against illegal content, including illegal products, online.

Johannes Heidelberger

The Bundesnetzagentur was appointed the Digital Services Coordinator (DSC) for Germany on 14 May 2024 with the entry into force of the German Digital Services Act (DDG), the national legislation implementing the DSA. The agency has been overseeing intermediary services and the implementation of the DSA in Germany since then.

The DSC of each EU Member State coordinates processes and information among relevant market players, including the intermediary services themselves, authorities, associations, companies, civil society organisations and recipients of the services.

The competence for supervising individual intermediary services lies initially with the Member State in which the provider of intermediary services has its main establishment or where its registered legal representative is located. Very Large Online Platforms and Very Large Online Search Engines (VLOPs/VLOSEs) are supervised by the European Commission itself.

The DSA provides various tools to support recipients of the service in their ability to take action against illegal content and products online. National DSCs are responsible for setting up these tools and monitoring compliance with them.

As such, DSCs carry out various certification processes including the certification of out-of-court dispute settlement bodies,

trusted flaggers, and researchers that have requested data access from VLOPs or VLOSEs.

Certified out-of-court dispute settlement bodies mediate between recipients and online platforms in cases where recipients are not satisfied with an online platform's decision about the removal of content or the disabling or deleting of an account. Certified trusted flaggers submit notices of presumed illegal content to online platforms, which have to prioritise looking into and processing them. Vetted researchers are granted the confirmed access to data of online platforms that they have requested and require to carry out their research into systemic risks and the mitigation of these.

The DSA also provides further options for recipients of the service to take action against illegal content on the internet, including requiring hosting services and online platforms to set up a reporting system on their services so that service providers can be informed of illegal content.

Recipients of the service and any body, organisation or association mandated to exercise the rights conferred by the DSA on their behalf have the right to lodge a complaint with the DSC of their own Member State against providers of intermediary services alleging an infringement of the DSA. Such complaints may only refer to breaches of the DSA and not to any identified presumed illegal content. The DSC itself does not monitor or remove content.

As the central point for complaints, the first step for the DSC upon receiving a complaint is to check whether it is actually responsible for dealing with it. In the event that the area of competence lies with a different DSC or the European Commission, it forwards the entire complaint to the relevant body. If the national DSC is competent to supervise the intermediary service in question, it is entitled to open national supervisory proceedings against the service provider.

The national DSC supports proceedings launched by the European Commission or other DSCs against providers of intermediary services if the authority leading the proceedings requests assistance, for example by collecting relevant information on the intermediary service under investigation from national actors and passing on their replies.

Providers of intermediary services that are found to be systemically in breach of the DSA in national and European supervisory proceedings face significant financial penalties.

The German DSC coordinates, but is not solely responsible for, the implementation of the DSA in Germany. Areas of competence have also been conferred by law on the media authorities of the federal states, the Federal Agency for Child and Youth Protection in the Media (BzKJ) and the Federal Commissioner for Data Protection and Freedom of Information (BfDI).

After more than a year's work as the DSC, we can conclude that the implementation of the DSA in Germany has got off to a good start. We have coordinated and communicated with market players, completed certification procedures, set up a complaint-handling system, initiated the first national proceedings and supported the European Commission in the proceedings it has launched. As we look to the years ahead, we remain focused on optimising our own processes as well as raising awareness of the DSA and its tools, especially among recipients of the services.

Johannes Heidelberger
heads the Digital Services Coordinator (DSC) at the Bundesnetzagentur in Bonn. He was previously Head of Section for Digitalisation, Online Networks and Internet Platforms.

ANDREAS LOBER / DANIEL TRUNK

Games in the EU's new platform law

A classification under the Digital Services Act

Consumer protection

In recent years, digital games have developed into complex social offerings on which players can create content, communicate and interact. This article examines the classification of such online games under the Digital Services Act. At the same time, the article provides an outlook on the resulting obligations and challenges for game providers. These are particularly challenging for online platforms.

reading time: 19 minutes

I. Introduction

With the Digital Services Act[1] (DSA), the EU broke new ground in the regulation of digital services. This comprehensive regulatory framework aims to create a safer and more transparent online environment and places particular emphasis on protecting consumers and safeguarding their fundamental rights.[2] Online games are facing new legal challenges.[3] They often allow players to interact with each other and to create new content.[4] They may thus fall within the scope of the DSA. In the following, we will examine what is important in this context.

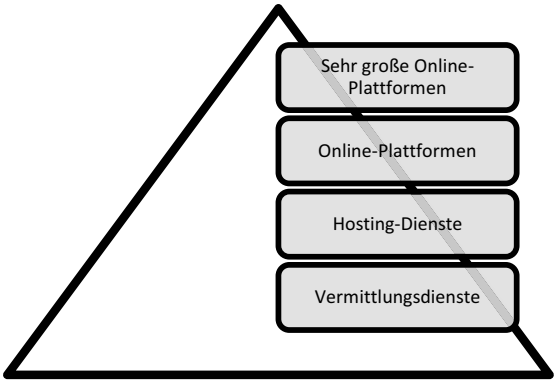
II. Scope of Application

The DSA comprises harmonised rules for the provision of intermediary services in the European Union (Art. 2 (2) DSA). The applicable rules and, in particular, the due diligence obligations depend on the nature, scope and type of the intermediary service.[5]

According to Art. 3 lit. g DSA, intermediary services can be classified into the following three different categories:

- Mere conduit services,
- Caching services and
- Hosting services.

In addition, the DSA highlights online platforms as a special form of hosting service (Art. 3 lit. i DSA). Further obligations apply to very large online platforms and very large online search engines. These are services that have an average of at least 45 million active recipients of the service per month in the EU and have been designated as such by the EU Commission (Art. 33 (1) DSA). To date, no online game has been designated as a very large online platform.



1. Online games as intermediary services

The DSA only applies to online games if they are "intermediary services".

a) Information society service

According to Art. 3 lit. g DSA, the first requirement for an intermediary service is that the service is an information society service (Art. 3 lit. a DSA). The reference in Art. 3 lit. a DSA to Art. 1 (1) lit. b Directive 2015/1535/EU[6] limits the scope of application to commercial services that are "generally provided for remuneration".[7] In practice, the requirements for such remuneration are low.[8] Online games, which are usually financed by purchase, subscription fees, in-game purchases or advertising,[9] regularly fall under this definition.[10]

b) Intermediary function

Another key feature of an intermediary service is its role as an intermediary of information provided by third parties without the service provider exercising control over this information.[11] Here, the understanding of the DSA is very broad. This is reflected in the term "illegal content" (Art. 3 lit. h DSA) which covers information regardless of its form, as long as it is potentially illegal or may be related to illegal activities.[12] For the online gaming sector, this means that games offering users opportunities for interaction and content creation could potentially be classified as intermediary services, regardless of whether this is achieved through content uploads, text input or playful elements such as a comprehensive level editor.

c) Mere conduit service

In case of a "mere conduit" service, information provided by a recipient of the service is merely transmitted via a communication network (Art. 3 lit. g sublit. i 1st Alt. DSA) This is a purely

1 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), OJ 2022 L 277, 1.
2 Recital 9 Sent. 1 DSA.
3 Trunk SpoPrax 2023, 329 (330); Nos. 46 and 47 of the Resolution of the European Parliament of 18 January 2023 on the single market approach for consumer protection in online video games (2022/2014(INI)), OJ 2023 C 214, 15.
4 No. 29 of the Resolution of the European Parliament of 18 January 2023 on the single market approach to consumer protection in online video games (2022/2014(INI)), OJ 2023 C 214, 159.
5 Recital 41 Sent. 1 DSA.
6 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on information society services, OJ 2015 L 241, 1.
7 Raue/Heesen NJW 2022, 3537.
8 Cf. Schmidt/Dreyer/Lampert, Spielen im Netz, 2008, p. 64, available at: https://www.hans-bredow-institut.de/uploads/media/Publikationen/cms/media/ad9293711df7ed3b6f4c4088d9e45dacc5559969.pdf.
9 Hentsch/Falk, Games und Recht/Anderie, 2023, § 17 marginal 21-26.
10 Trunk SpoPrax 2023, 329; see also for the German concept of telemedia: Fezer/Büscher/Obergfell, Lauterkeitsrecht: UWG/Mankowski, 3rd ed. 2016, p. 12 marginal 163a.
11 Hofmann/Raue, Digital Services Act/F. Hofmann, 2023, Art. 3 marginal 45.
12 Recital 12 Sent. 3 DSA.

technical process of information transmission. The provider is not the creator of the content and does not modify the content during the transmission.[13]

d) Hosting service

A hosting service stores information provided by a recipient of the service on the recipient's behalf (Art. 3 lit. g sublit. iii DSA).

e) Online platform

If the service meets the requirements of a hosting service, the question then is whether it is an online platform which entails further extensive obligations. An online platform is legally defined as a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation (Art. 3 lit. i DSA).

In simple terms, an online platform within the meaning of Art. 3 lit. i DSA stores and disseminates the information provided by a recipient of the service publicly on behalf of the recipient whereas this function must not be of a merely ancillary nature.

Art. 3 lit. k DSA defines dissemination to the public as making information available to a potentially unlimited number of third parties at the request of the recipient of the service who provided the information. It is sufficient that the information is easily accessible to a potentially unlimited number of recipients of the service, irrespective of whether those persons actually access the information in question.[14] The need for a log-in is harmless if registration is automatic, i.e. basically open to everyone.[15] Many online games allow such automatic registration which indicates that the criterion of publicity is met. Public dissemination can be assumed if, for instance, user-generated content can be made visible to other recipients of the service within the game.

A limiting factor is whether public dissemination only plays a subordinate role in the overall context. This is intended to avoid overly broad obligations.[16] The decision on the application of this exception requires a case-by-case assessment while the DSA only roughly outlines the legal framework. The comments section of an online newspaper should be regarded as a secondary function since it is clearly subordinate to the main service – the publication of news under the editorial responsibility of the publisher.[17] In contrast, the storage of comments in a social network should be considered an integral part of an online platform as it is obviously not an ancillary function of the service offered, even if it serves the contributions of the recipients of the service.

2. Evaluation of individual game elements

The following non-exhaustive (partly technical) classification focuses on the specific features and interaction options that are frequently included in online games.

a) Chat functions

If players communicate via voice or text channels in the game, the provider transmits third-party user information. These functions can be classified as mere conduit services or hosting services, depending on how the communication takes place technically.

The DSA classifies both voice over IP and interpersonal communications services as "mere conduit". Interpersonal communications services within the meaning of Art. 2 No. 5 of the Directive on the European Electronic Communications Code (EECC Directive) are characterised by the fact that they enable a direct and interactive exchange of information between a finite number of persons, whereby the recipients are determined by the persons who initiate or are involved in the communication. In addition to group chats, the EECC Directive also mentions communication channels in online games in Recital 17 of the EECC Directive.

If the chats are stored, they may be classified as hosting services (Art. 3 lit. g sublit. iii DSA). However, the storage of chats in online games does not generally lead to classification as an online platform pursuant to Art. 3 lit. i DSA, as the chats are usually not publicly disseminated. Such dissemination would involve making information available to an unlimited number of third parties which is not the case with interpersonal communication between limited groups of recipients of the service.[18] Public dissemination may be the case, for instance, with public groups or open channels.[19]

b) Gameplay

When participating in an online game, information is also transmitted to fellow players and opponents. In online chess, for instance, a player's move is transmitted to the opponent via the server. In an online shooter, on the other hand, real-time data such as the position, status (e.g. health points, equipment) and actions (e.g. shots, movements) of all players must be synchronised via the server and transmitted to the respective clients of the other players. The question arises as to whether the gameplay itself leads to the online game being classified as an intermediary service. Holznagel argues in favour of such a classification even in the case of merely fleeting gameplay as even actions such as insults must be stored on the online servers for a short time.[20] This opinion, however, in its generalisation, lacks a more detailed consideration of the individual technical functions.

As already mentioned, certain communication channels such as voice over IP do not require the fleeting storage of user information. Furthermore, in the opinion of the authors, the mere playing of a game does not constitute the storage or dissemination of third-party information, as required by the DSA: An online sports simulation or a purely competitive battle royale shooter would seem to be miles away from the services for exchanging information and content that the legislator had in mind in Recital 29, sentence 4 of the DSA. What is and is not possible within the game is specifically defined by the game programme.

Classification as an intermediary service is also not appropriate in terms of wording and purpose. The term "information" which is decisive for opening the scope of application is not legally defined either in the DSA or in the E-Commerce Directive[21]. The English[22] and French[23] versions also lack any indication of its meaning under EU law. However, the DSA suggests a difference between "information" and "content" as it uses both terms, e.g. in the definition of "content moderation". If one compares

13 Gersdorf/Paal, BeckOK Informations- und Medienrecht/Hennemann, 46. ed 2023, TMG § 8 marginal 14.
14 Recital 14 Sent. 1 DSA.
15 Recital 14 Sent. 2 DSA.
16 Recital 13 Sent. 3 DSA.
17 Recital 13 p. 4 and 5 DSA.
18 Recital 14 Sent. 3 DSA.
19 Recital 14 Sent. 4 DSA.
20 Müller-Terpitz/Köhler, DSA/Holznagel, Art. 3 marginal 89.
21 Directive (EC) 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ 2000 L 178, 1.
22 Information provided by the recipient of the service.
23 Informations fournies par un destinataire du service.

the DSA with other digital acts such as the Data Act[24], the term "information" appears less comprehensive than the term "data".[25] However, it should be noted that the Data Act pursues a different objective than the DSA with its concept of fair access to data, which could be an argument against a uniform understanding of the term.[26] Looking at the purpose of the DSA, it aims to create a secure, predictable and trustworthy online environment that counteracts the spread of illegal online content and social risks such as disinformation.[27] In principle, these risks cannot be transferred to pre-programmed game interactions: In most online games, the computer programme limits the possibilities for play to such an extent that (illegal) content or information addressed by the DSA cannot commonly arise from the mere gameplay. In this respect, the game itself is more comparable to an interactive movie (e.g. Black Mirror: Bandersnatch[28]). If the DSA's understanding of the term were so broad that even the pressing of a button or a simple selection of pre-configured options is information provided by the recipient of the service within the meaning of the DSA, every saving of settings in an online service would also have to be classified as a hosting service. This would lead to considerable over-regulation, the usefulness of which is questionable.

c) User-generated content and virtual identities

Online games often provide creative freedom by allowing users to generate their own content. This ranges from designing avatars or vehicle bodies to creating entire game worlds. In addition, recipients of the service often have the option of personalising their profile with a username of their choice and, if desired, additional information such as text. Some games also allow users to design their own logos that are visible in the game.[29] This content may be illegal or violate the rules of the Game Licence Agreement with the publisher. By storing this content, the publisher generally provides a hosting service in accordance with Art. 3 lit. g sublit. iii DSA.

d) Overall assessment

If, according to the criteria outlined above, information provided by users is publicly disseminated, this constitutes an online platform, so long as it is not a minor secondary function. Here, it must be determined what the main function of the service is.

In general, the purpose of online games is to enjoy the gaming experience. Competitive games are primarily about competing against each other, while story-based role-playing games focus on solving tasks (often together) and experiencing the story. The game functions can be as wide-ranging as they are varied. However, in some online games such as Roblox[30] or Minecraft[31], the focus is much more on user-generated content. In these games, users can create entire worlds and share them with other users. The more the focus is on these functions, the less room there is for arguing against classifying it as an online platform.

III. Due diligence obligations under the DSA

The DSA's due diligence obligations are so detailed that they could fill entire chapters or even books. Thus, we will focus on the characteristics of online games below.

For an initial understanding, it is helpful to bear in mind that the DSA sets out basic obligations for all providers of intermediary services and additional obligations for providers of hosting services, in particular for providers of online platforms and very large online platforms. The due diligence obligations set out in this section are not exhaustive.

1. Terms and conditions

One of the DSA's key demands is transparency when it comes to content restrictions imposed by the intermediary service. The DSA identifies the general terms and conditions (GTC) of the intermediary services as one of the main sources of information on restrictions.[32] According to Art. 14 DSA, these must disclose certain parameters regarding the moderation of content, regardless of the type and size of the intermediary service. Unlike other obligations, such as the requirement for annual transparency reports (Art. 15 DSA), there is no exception for small or micro enterprises.[33]

Content moderation describes the activities – automated or non-automated – that are intended in particular to identify and address content or information provided by recipients of the service that is illegal or incompatible with the terms and conditions (Art. 3 lit. t DSA). This includes measures that affect the availability, display and accessibility of this information.

Many online games already contain rules of conduct in their end-user licence agreements[34] or other guidelines[35]. These rules of conduct can be considered terms and conditions.[36] The DSA provides a clear and predictable legal framework for the moderation of content for recipients of the service.[37] Providers must thus ensure that they provide the corresponding information as specified and required by the DSA.

Vague clauses in terms and conditions, such as non-exhaustive lists of prohibitions, are problematic. These phrases offer no added value to providers under the DSA as they are required to disclose all restrictions and discriminatory moderation of cases outside the scope of the GTC should be avoided as a matter of principle.[38] More abstract terms such as hate speech may be permissible, especially if they are backed up with examples.[39] Game-specific technical terms that are familiar to the target audience may be used[40] but less familiar terms should be explained in a way that a broad audience can understand.

The DSA requires information on measures and tools that can be used to detect and identify undesirable content. This includes human review as well as tools used for automated moderation of content. These tools also include simple solutions such as word filters that suppress swear words in chat, for example, according to a list provided by the publisher. The reporting and action mechanism provided for in Art. 16 DSA can also be seen as a tool for restricting content.[41]

24 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules for fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Regulation), OJ 2023 L, 2023/28549.
25 Data are defined in Art. 2 No. 1 DA as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual material".
26 Recital 5 DA.
27 Recital 9 Sent. 1 DSA.
28 "Black Mirror: Bandersnatch" is a movie released on Netflix in which viewers can determine the direction of the plot several times by making selection decisions.
29 A well-known example is the emblem generator which can be found in various Call of Duty games or in Armored Core VI™: Fires of Rubicon™, among others.
30 Roblox is a gaming platform developed by Roblox Corporation.
31 Minecraft is a sandbox computer game developed by Mojang Studios.
32 Hofmann/Raue, Digital Services Act/F. Hofmann,2023, Art. 1 marginal 22.
33 ZB Art. 15 (2) DSA.
34 Maties, Stichwortkommentar eSport-Recht/Picot, 2023, p. 48 marginal 2.
35 E.g. the Rocket League Code of Conduct, available at: https://www.rocketleague.com/de/news/rocket-league-code-of-conduct.
36 BGH MMR 2017, 394 51 et seq.; Hentsch/Falk, Games und Recht/Sestner/Kaster, 2023, marginal 22.
37 Recital 47 p. 1 DSA; Raue/Heesen NJW 2022, 3537 (3540).
38 Hofmann/Raue, Digital Services Act/Raue, 2023, Art. 14 marginal 3; Schwartmann NJW 2022, 133 (134); Raue/Heesen NJW 2022, 3537 (3540).
39 OLG Dresden MMR 2018, 756marginal 13 et seq.
40 BGH MMR 2017, 394 marginal 63; Trunk SpoPrax 2022, 216 (218); Maties/Püschel SpoPrax 2022, 306 (308).
41 No. 8 of the ZeniMax Media Terms of Service, available at: https://www.zenimax.com/de/legal/terms-of-service.

The DSA does not provide any further details on tools for anti-cheating measures. When cheating, the cheater usually manipulates the programme flow and thereby gains a gaming advantage,[42] for instance by automatically aiming[43] or being able to see through walls[44]. However, players do not usually provide their own information within the meaning of the DSA simply by using cheats while playing (see II.2.b)).

2. Transparency reports

All service providers are obliged to publish a transparency report at least once a year, unless they are considered micro or small enterprises (Art. 15 (1) sent. 1 DSA). These transparency reports must contain information on the official orders they have received (lit. a), meaningful and comprehensible information on content moderation carried out on their own initiative (lit. c) and the number of complaints received via the internal complaint management systems in accordance with the service provider's general terms and conditions (lit. d). Providers of hosting services, online platforms and very large online platforms are obliged to provide further information in their transparency reports.

The EU Commission has issued an implementing regulation pursuant to Art. 15 (3) DSA to define a binding model for the form and content of the transparency reports and to harmonise the reporting periods.[45] These models seem quite inappropriate for most online games.

3. Notice and action mechanism for hosting services

Providers of hosting services, including online platforms, regardless of their size, must put in place an easily accessible and user-friendly notice and action mechanism that enables individuals and entities to report information they consider to be unlawful (Art. 16 (1) DSA). Many details are regulated in Art. 16 DSA. Among other things, the procedure should be easily accessible for everyone, i.e. not only for the recipients of the service but also for third parties, e.g. authorities.[46] Since the reporting function should also be located in proximity to the information to be reported[47], the requirements for online games are not easy to be met because there is a conflict between the requirement that the reporting option be located close to the information being reported (i.e., reporting option directly in the game) and free accessibility for all (i.e., without registration). To gain access to the game (and thus a reporting and action mechanism in proximity of the possibly problematic information), every recipient of the service generally requires a corresponding license which in practice usually requires registration (and/or the conclusion of a game licence agreement). It becomes clear that the specific characteristics of online games are not adequately addressed by the rather rigid provisions of Art. 16 DSA.

4. Recommender systems

Providers of online platforms that use so-called recommender systems must set out the main parameters of these systems in their terms and conditions in plain and intelligible language, as well as all options available to recipients of the service to modify or influence these main parameters (Art. 27 (1) DSA). Recommender systems, defined more precisely in Art. 3 lit. s DSA, are filtering tools that are intended to help recipients of the service prioritise the content presented to them.[48] In the case of online games, this is relevant, for instance, when various user-generated content is suggested in a catalogue. The transparency obligation serves to inform recipients of the service why certain user-generated content is being offered to them.

5. Disclosure of active recipients of the service

In addition to other transparency reporting obligations, online platforms are obliged to publish the average number of their monthly active recipients of service in the European Union at least every six months (Art. 24 (2) DSA). This key figure is relevant because online platforms with more than 45 million active recipients of the service are classified as very large online platforms and as such are subject to numerous other due diligence obligations and supervision by the EU Commission. The monthly average number of active recipients of the service should reflect all recipients of the service who have actually used the service at least once by being exposed to the information disseminated via the online interface of the online platform, e.g. by viewing, listening to or providing information.[49] Reliably determining these figures is generally difficult due to data protection regulations on user tracking. If a game consists of several different parts, not all of which can be classified as online platforms, the authors believe there are good arguments for using the number of only these users as the relevant benchmark rather than the total number of active players of the game. In this case, only those players who have accessed the respective online platform part of the game are exposed to information from the online platform so that the other players are not at risk of potentially illegal third-party content.

5. Minors

The DSA contains special provisions for the protection of minors in several places. In Germany, these are enforced by the Office for the Enforcement of Children's Rights in Digital Services (KidD) which is part of the Federal Agency for Child and Youth Media Protection (BzKJ).[50] If an intermediary service is primarily aimed at minors or is predominantly used by minors, the provider must explain the conditions and restrictions for using the service in a way that minors can understand (Art. 14 (3) DSA). This can be assumed if more than 50% of recipients of the service are minors.[51] Providers may consider using graphic elements such as icons or images in their terms and conditions to illustrate the essential elements of the information obligations.[52]

Online platforms that are accessible to minors must take appropriate and proportionate measures to ensure a high level of privacy, safety and protection for minors on their service (Art. 28 (1) DSA).[53] Targeted advertising to minors is prohibited (Art. 28 (2) DSA), i.e. – in contrast to the GDPR – not even permitted on the basis of consent.

IV. Outlook

The introduction of the DSA poses new legal challenges for providers of online games. Due to their interactive and social nature, they may fall within the scope of the DSA, especially if they store user-generated content and share it with other players. This may require a detailed review and, if necessary, adaptation of the game

42 Nothelfer/Trunk SpoPrax 2022, 341.
43 So-called aim bots.
44 So-called wall or map hacks.
45 Implementing Regulation (EU) 2024/2835 of the Commission of 4 November 2024 laying down templates for transparency reporting obligations of providers of intermediary services and online platform providers under Regulation (EU) 2022/2065 of the European Parliament and of the Council. OJ L, 2024/2835.
46 Spindler GRUR 2021, 545 (552); Hoffmann/Raue, Digital Services Act/Raue, 2023, Art. 16 marginal 16.
47 Recital 50 Sent. 3 DSA.
48 Hofmann/Raue, Digital Services Act/Grisse, 2023, Art. 27 marginal 13.
49 Recital 77 Sent. 2 DSA.
50 Cf. Terhörst MMR 2024, 525.
51 Kraul, Das neue Recht der digitalen Dienste/Maamar, 2022, § 4 marginal 43; Hofmann/Raue, Digital Services Act/Raue, 2023, Art. 14 marginal 70.
52 Recital 45 Sent. 5 DSA.
53 See also von Petersdorff MMR 2025, 669 – in this issue.

to meet the new legal requirements. Such requirements always entail a great deal of additional work which poses economic challenges for smaller game providers in particular. At the same time, there are still no clear, binding guidelines for some due diligence obligations as to how these can be sensibly (!) implemented in online games. So, it remains to be seen how providers will implement this and how authorities will monitor it in the coming months and years. After all, the success of the DSA will be measured by the extent to which it is enforced in the EU Member States.

Quick read ...

- The classification of online games under the DSA depends on their features and technical implementation. In particular, games with interactive features such as communication and user content should be examined.
- According to the opinion expressed here, unlike chats or user-generated content, the actions of players in the normal course of the game do not generally constitute 'third-party information' passed on by the game provider.
- The due diligence obligations under the DSA bring new challenges for publishers. There is a need for action in the GTC, among other things.
- The requirements for the notice and action mechanism for hosting services only make sense for online games to a limited extent.

Dr Andreas Lober
is a lawyer and partner at ADVANT BEITEN in Frankfurt/Main and head of the IP/IT/Media practice group.

Daniel Trunk
is a lawyer at ADVANT BEITEN in Frankfurt/Main.

LORENZO VON PETERSDORFF

Online protection of minors under the DSA

Implications of the EU guidelines for the games industry

Standards of protection

With Article 28 of the DSA, the EU is establishing a structural framework for the protection of minors on online platforms for the first time. The current draft guidelines from the EU Commission specify the obligations of providers, but their implementation poses challenges in terms of legal certainty and practicability, including for the games industry. This article provides an overview of the legal framework and analyzes key aspects of the draft from the perspective of the Entertainment Software Self-Regulation Body (USK), including the basic principles and selected measures. It shows that the strong focus on technical age verification is at the expense of other proven instruments. Questions regarding the system, unclear terminology, and the impression of de facto obligations make coherent implementation difficult. The article argues for a risk-oriented, proportionate application involving proven and existing (self-regulatory) approaches. reading time: 24 minutes

I. Introduction

The protection of minors is an important political objective of the EU.[1] This is primarily manifested in the provisions of Article 28 of Regulation (EU) 2022/2065 (DSA), which establishes the protection of children and young people at the level of platform regulation. Online platforms have become central spaces for minors to gain experience and communicate. On the one hand, they offer access to educational opportunities, social participation, and creative development, but at the same time they harbor a multitude of risks, such as communication and contact risks, problematic content, manipulative design elements, or the integration of AI-based interaction systems. In the gaming industry, there are also relevant offerings that may fall under the definition of an online platform within the meaning of Article 3(i) DSA.[2] Some gaming platforms are already much more than mere distributors; they also offer extensive opportunities for interaction, communication, and the creation and sharing of user-generated game worlds without in-depth programming knowledge.[3] The need for legally binding safeguards arises in particular from the primary law guarantees of the GRCh. Minors deserve special consideration in this regard, as protection, empowerment, and participation rights are particularly relevant in the context of their development into mature individuals, as also stated in the 25th General Comment on the UN Convention on the Rights of the Child in digital environments.[4] From the perspective of the Entertainment Software Self-Regulation Body (USK) as a "one-stop shop" for youth media protection in the gaming sector in Germany, this article provides an overview of the legal framework and the opportunities and challenges of a

1 Cf. Recital 71 DSA p. 1.
2 In detail, cf. Lober/Trunk MMR 2025, p. 565 ff. – in this journal.
3 Cf. USK press release dated January 15, 2025, regarding "Game Creator Plattformen auf dem Prüfstand: Änderung der Alterskennzeichen bei unzureichendem Jugendschutz", available at: https://usk.de/game-creator-plattformen-auf-dem-pruefstand-aenderung-der-alterskennzeichen-bei-unzureichendem-jugendschutz/.
4 Cf. Mast/Kettemann/Dreyer/Schulz, Digital Services Act, 2024, Art. 28 mn. 2.

differentiated, risk-based implementation of the due diligence obligations under Art. 28(1) DSA. The focus is on the current draft of the guidelines published by the EU Commission pursuant to Art. 28(4) DSA, the main content of which is presented in overview and in greater detail in selected aspects.[5]

II. Systematics of online protection for minors under the DSA

Pursuant to Article 28(1) of the DSA, providers of online platforms accessible to minors are required to take appropriate and proportionate measures "to ensure a high level of privacy, safety, and security of minors on their service". In order to assist online platform providers in applying Section 1 and the undefined legal terms contained therein, the Commission may issue guidelines (see III.). Germany has made use of the provision in Art. 49(2) subsection 1 sentence 2, so that the Federal Agency for the Protection of Children and Young People in the Media (BZKJ) or the Federal Office for the Enforcement of Children's Rights in digital Services (KidD) pursuant to § 12(2) DDG has been designated as the competent authority for the enforcement of structural precautionary measures under Article 28(1) DSA, insofar as measures under the Interstate Treaty on the Protection of Minors in the Media (JMStV) are not affected.[6]. The state authorities are responsible for these specific individual measures under the JMStV. Sections 2 and 3 of Article 28 DSA contain data protection requirements: Section 3 prohibits platforms from displaying personalized advertising based on profiling (Article 4(4) GDPR) to users if they are minors with sufficient certainty. At the same time, it clarifies that no additional personal data may be processed for the purpose of determining age in order to comply with Article 28 DSA, as the principle of data minimization (Article 5(1)(c) GDPR) also applies to measures under Section 1. The competent authority is the Federal Commissioner for Data Protection and Freedom of Information (BfDI; § 12(3) DDG). [7]

1. Addressee of Article 28 (1) DSA

a) Online-Platform

Article 28 DSA addresses online platforms within the meaning of Article 3(i) DSA and thus a subcategory of hosting services. Unlike "pure" hosting services, which store information provided by a user on their behalf, online platforms are characterized by the fact that they publicly disseminate content or information. However, if storage and dissemination are merely a secondary function, the service does not constitute an online platform. This exception, which is likely to be significant in practice, applies if the function is merely ancillary to another service or an insignificant function of the main service which, for objective and technical reasons, cannot be used without that other main service.[8] This also includes a corresponding prohibition on circumvention. Film and gaming platforms within the meaning of the national regulation of § 14a JuSchG are therefore not covered, provided that the main service does not comprise the provision of third-party content for individual retrieval, but rather its own content (e.g., platforms for the PlayStation, Xbox, Nintendo Switch, etc.). If these platforms only provide supplementary communication functions (player chat) or sharing functions of a minor nature (e.g., game snapshot sharing) in addition to their main function in the form of extensive own content, the services are still not to be classified as online platforms.[9] However, this is to be assessed differently in the case of offers such as the Roblox platform. Furthermore, the provision of Art. 28 DSA does not apply to providers of online platforms that are classified as micro or small enterprises in accordance with Recommendation 2003/361/EC.[10] Regardless of their size and turnover, very large online platforms (VLOPs) within the meaning of Article 33 DSA are always subject to due diligence obligations pursuant to Article 19(2) DSA.

b) "Platforms accessible to minors"

According to Art. 28 (1) DSA, only online platforms that are "accessible to minors" are covered by its scope. Minors are defined as persons under the age of 18.[11] According to recital 71 of the DSA, online platforms fall under this characteristic if their "terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes." The wording gives the impression that these criteria are alternatives. This would mean that the rule in Article 28(1) DSA wouldn't apply if the platform's terms and conditions only let adults use it, even if the platform is mostly used by minors. However, in line with the broad wording of the provision, the EU Commission has clarified in its draft guidelines pursuant to Article 25(4) DSA that the mere possibility of accessing the respective online platform is sufficient to bring it within the scope of application. [12] Offers that are exclusively accessible to adults cannot therefore be covered by the scope of application, for example on the basis of document-based and personally identifiable age verification (AVS) as used in the context of national youth protection standards pursuant to Section 4 (2) sentence 1 no. 1, sentence 2 JMStV.[13]

2. Measures

The term "measure" within the meaning of Article 28 DSA must be interpreted broadly. It covers all actions, precautions, and arrangements, including technical functions, procedures, and processes, or cooperation with external third parties, which are primarily preventive in nature and relate to the service. In addition, forms of documentation or accompanying information-related activities, such as information campaigns or evaluations, as well as measures that take effect after a risk has materialized and can mitigate it, are also covered.[14] According to Art. 28(1) DSA, measures must be appropriate and proportionate. This means that they must have a positive impact on the protective dimensions of privacy, safety, and security, and the effort involved must be proportionate to the risk reduction sought. The higher the potential harm to minors posed by an online service, the more comprehensive the protective measures to be taken. Since different online platforms pose different risks to minors, each case must be examined individually. In

5 EU Commission, press release dated May 13, 2025, on "Commission guidelines on measures to ensure a high level of privacy, safety and security for minors online pursuant to Article 28(4) of Regulation (EU) 2022/2065" (Draft guidelines), available at: https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act.

6 Cf. Terhörst MMR 2024, 525.

7 BeckOK JugendschutzR /Liesching, 4th ed. 1.12.2024, DSA Art. 28 mn. 55.

8 Examples can be found in recital 13, subparagraph 1, sentence 4 et seq. (comment section of an online newspaper; web hosting) and counterexamples (dissemination of comments on social networks).

9 BeckOK JugendschutzR /Liesching, 4th ed. 1.12.2024, DSA Art. 28 mn. 6.

10 The current thresholds are less than 50 employees and an annual turnover not exceeding EUR 10 million for small enterprises. For micro-enterprises, the thresholds are less than 10 employees and an annual turnover not exceeding EUR 2 million.

11 Cf. clarification in footnote 1 of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025, available at: https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act.

12 Cf. line 53 et seq. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025, available at: https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act.

13 Mast/Kettemann/Dreyer/Schulz, Digital Services Act, 2024, Art. 28 mn. 41.

14 Mast/Kettemann/Dreyer/Schulz, Digital Services Act, 2024, Art. 28 mn. 45.

accordance with the EU Commission's draft guidelines, the type and nature of the services offered by the provider, the intended or current use, and the user base of the service must be taken into account. In addition, the provider must examine any infringements of fundamental rights, in particular with regard to the rights of minors under the GRCh.[15] The proportionality based on the assessment of such a cost-benefit ratio, which must also take into account the human, technical, and economic resources required by the provider, reaches its limits where the requirements for due diligence become so high that the continued operation of the service is no longer feasible or only feasible with considerable difficulty.[16] The underlying standard is a "high level," whereby all measures implemented must be taken into account in this assessment. Although this wording implies a fundamentally ambitious understanding, it also makes it clear that the highest degree does not have to be achieved in order to enable minors to grow up in the digital environment as unimpeded as possible..[17]

III. Commission guidelines pursuant to Article 28 (4) DSA

The Commission may, after consulting the Committee, issue guidelines to "assist" online platform providers in applying Article 28(1) DSA. Accordingly, the guidelines are not legally binding, but they do provide guidance and an important benchmark that the Commission will use when applying Article 28(1) DSA, so that they have a rule-clarifying regulatory character in the context of administrative or judicial proceedings. In addition, online platforms supervised by the BzKJ and based in Germany must give priority to the guidelines over the list of examples in Section 24a(2) of the JuSchG..[18] However, implementation of the guidelines does not constitute "automatic" compliance, as the interpretation of the provision is ultimately reserved for the European Court of Justice. A draft of the guidelines was published in May 2025 [19] and submitted for public consultation. Although the final version is still pending, the draft already provides a high degree of certainty regarding the basic approach of the future guidelines.

In particular, the guidelines comment on general principles to be taken into account that are to apply to all measures within the meaning of Article 28(1) DSA. In addition to (1) the principle of proportionality (see II. 2.), (2) consideration of the rights of the child (including the right to protection, non-discrimination, inclusion, participation, privacy, information, and freedom of expression), (3) privacy, safety, and security-by-design ("highest" standards in the design, development and operation of their services), and (4) age-appropriate design (alignment with the developmental, cognitive, and emotional needs of minors while ensuring their privacy, security, and protection) are explained. The report then lists the key measures that the Commission believes providers should take to ensure a high level of privacy, safety, and security. These include risk review, service design, and [20] , reporting, user support and tools for guardians ter[21] and governance [22]. It is clarified that the measures described are not exhaustive. For example, measures resulting from compliance with other EU legislation or national guidelines on the protection of minors are also possible.[23] Within the individual sections, some very specific ideas are set out.

The guidelines supplement the provisions of the DSA, in particular regarding the due diligence obligations for VLOPs and VLOSEs (Very Large Online Search Engines) pursuant to Art. 33 et seq. DSA, on notification and redress procedures (Art. 16 ff. and 20 ff. DSA) or transparency obligations (Art. 14 f. and 24 DSA) and build on existing obligations without interpreting or replacing them. Providers must therefore independently assess whether additional measures are necessary. Art. 28(1) DSA must also be understood in the context of other EU law requirements for the protection of minors in the digital space. Although the guidelines are primarily aimed at minors, they may also increase the protection of all users.[24]

1. Risk Review

Risk assessment is central to the implementation of Article 28(1) DSA. It is based on a structured analysis that, in accordance with the guidelines, covers at least the following points: [25]

- Firstly, the likelihood of minors using the platform must be assessed.
- Secondly, the associated risks must be identified using the "5Cs" typology, which, according to German youth protection law, can be divided into the risk areas of confrontation (content risks), interaction (contact and conduct risks), and other usage risks (consumer and cross-cutting risks). Aspects such as purpose, design, marketing, functions, the number and type of users, and the actual and expected uses may be relevant here.
- Thirdly, existing and potential additional measures to minimize risk should be examined. In doing so, it must always be assessed whether the measures are proportionate to the risk being mitigated. However, possible negative effects on children's rights, in particular with regard to participation in the digital environment, freedom of expression, and the right to information, are also explicitly mentioned. The risk assessment should also be carried out in the light of the best interests of the child and updated whenever the online platform's service undergoes significant changes, with publication of the results recommended. Existing instruments such as the Child Rights Impact Assessment [26] can be used to support the risk review.

2. Age Assurance

Age assurance measures are a central aspect of the guidelines. According to the guidelines, age assurance refers to all measures that regulate access to online services based on age in order to protect minors from inappropriate online content[27] There are three categories: "Self-Declaration," "Age Estimation," and "Age Verification." Self-Declaration is based on voluntary information provided by users and, according to the guidelines, is not reliable enough to meet the requirements of Art. 28 (1) DSA.

15 Cf. line 147 ff. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.
16 Mast/Kettemann/Dreyer/Schulz, Digital Services Act, Art. 28 DSA mn. 56.
17 Cf. Müller-Terpitz/Köhler/Holznagel, 2024, DSA Art. 28 mn. 24.
18 Cf. BeckOK JugendschutzR /Liesching, 4th ed. 1.12.2024, DSA Art. 28 mn. 56.
19 EU Commission, press release dated May 13, 2025, available at: https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act.
20 Among them: "6.1 Age assurance"; "6.1.1 Introduction and terminology"; "6.1.2 Determining whether to put in place age assurance measures"; "6.1.3 How to choose and implement age assurance measures".
21 Among them: "7.1 User reporting, feedback and complaints"; "7.2 User support measures"; "7.3 Tools for guardians".
22 Among them: "8.1 Internal processes and oversight"; "8.2 Training and awareness"; "8.3 Monitoring and evaluation"; "8.4 Transparency".
23 Cf. line 138 f. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.
24 Cf. line 87 ff. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.
25 Cf. line 174 ff. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.
26 Available at: https://www.nldigitalgovernment.nl/document/childrens-rights-impact-assessment-fill-in-document/.
27 Cf. line 210 et seq. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.

Age estimation provides a probability forecast of age based on technical methods (e.g., AI-supported analysis), while age verification relies on verified and secure sources of identification (e.g., government ID) and promises a high degree of accuracy. A proportionality assessment must be carried out to determine whether age assurance is necessary for the risks posed by the service in question. "In this regard, the Commission is of the view that providers should also consider other measures set out in other sections of these guidelines as an alternative to age assurance measures."[28]

Specifically, according to the current opinion of the EU Commission, age verification is appropriate in the following circumstances:

- EU or national law prescribes a minimum age for access to certain services or content (e.g., sale of alcohol, gambling, pornography)
- terms of use or other contractual obligations set an age limit of "18 years or older" in order to exclude minors due to identified risks,
- other circumstances exist in which a risk assessment by the provider indicates that there are high risks for minors (including contact and content risks) that cannot be mitigated by less restrictive means.

Age estimation is then considered appropriate if

- the terms of use or similar contractual obligations of the service require that a user must be at least 18 years of age to access the service and specify the provider's assessment of when the online platform can be used safely by minors,
- the platform only poses "medium risks" and these cannot be mitigated by less restrictive measures.[29]

Before introducing any of these age estimation methods, providers should consider whether they meet broadly defined standards of accuracy, reliability, circumventability, privacy-friendliness, data minimization, and low intrusiveness, as well as non-discrimination. The future EU Digital Identity Wallet (EUid) is intended to provide such a standard.[30] In addition, at least two different methods for age verification or estimation and a complaint mechanism in the event of incorrect age determination must be available, which in turn must comply with the requirements of Art. 20 DSA.[31]

3. Tools for Guardians

Tools for guardians are also included in the draft guidelines. These include digital features or applications that help parents and guardians manage their children's online activities, privacy, and well-being, e.g., through screen time limits, spending restrictions, or account settings management.[32] The Commission clarifies that such tools should be considered only complementary to other safeguards under Article 28(1) of the DSA. They should not be the sole safeguard to ensure a high level of privacy, safety and security, nor should they replace other measures taken for this purpose. However, it is noted that they can contribute to such a high level in combination with other measures. In addition, the specific aspects that such tools should ensure are specified in more detail. [33]

4. Default settings

According to the guidelines, default settings play a key role in protecting minors on online platforms, as they are not changed by most young users and therefore significantly shape their user experience. The Commission therefore considers that online platforms accessible to minors and "that use default settings to ensure a high level of privacy, safety, and security of minors on their service for the purposes Art. 28(1) [DAS]" , should meet more specific requirements. In particular, it is emphasized that children's accounts must be designed from the outset to provide the "highest" level of protection possible. Specific requirements include restrictive communication options, the deactivation of sensitive functions (e.g., geolocation or camera), and protection against excessive use (e.g., by disabling push notifications or deactivating likes). Such default settings should be reviewed regularly, include age-appropriate explanations, and not encourage users to lower the level of protection.[34]

5. Commercial Practices

The guidelines emphasize that minors are particularly vulnerable to the mechanisms of commercial practices and therefore require special protection from economic exploitation. Despite this need for protection, minors in the digital space are regularly exposed to diverse, dynamic, and personalized advertising strategies-for example, in the form of advertising, product placements, in-app currencies, influencer marketing, or AI-supported "nudging."[35] Against this background and without prejudice to further specific provisions of the DSA – in particular on advertising (Articles 26 and 28(2) DSA) and on the prevention of "dark patterns" (Art. 25 DSA) – the Commission recommends a series of supplementary measures that should be taken to comply with Art. 28(1) DSA. Some of these measures directly address the medium of "games" or may be relevant to games. The guidelines mention, for example, "ensuring the transparency of economic transactions in an age-appropriate manner and avoiding the use of virtual intermediate currencies such as tokens or coins that can be exchanged for real money and then used to purchase other virtual items, which can reduce the transparency of economic transactions and be misleading for minors." The guidelines mention, for example, "ensur[ing] transparency of economic transactions in an age-appropriate way and avoid the use of intermediate virtual currencies, such as tokens or coins, that can be exchanged with real money and then used to buy other virtual items, which can have the effect of reducing transparency of economic transactions and may be misleading for minors". [36] It is also necessary to "ensure that minors are not exposed to practices that may lead to excessive or unwanted spending or addictive behavior by ensuring that virtual items such as loot boxes, other products with random or unpredictable outcomes or gambling-like features are not accessible to minors, and by introducing separation or friction between content and the purchasing of related products."[37] In addition, there are other aspects, such as ensuring "that minors are not exposed to manipulative design techniques such as scarcity, intermittent or random rewards" , or ensuring "that minors are not exposed to unwanted purchases, e.g. by considering deploying effective tools for guardians". The labeling of advertising content and the direct targeting of minors in advertising are also mentioned.

28 Cf. line 235 et seq. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.
29 Cf. line 247 et seq. of the draft guidelines pursuant to Art. 28 (4) of the EU Commission of May 13, 2025.
30 Cf. line 268 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.
31 Cf. line 256 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.
32 Cf. line 841 et seq. and 864 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.
33 Cf. line 253 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.
34 Cf. line 383 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.
35 Cf. line 612 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.
36 Vgl. Zeile 653 ff. des Entwurfs der Leitlinien gem. Art. 28 Abs. 4 der EU-Kommission v. 13.5.2025.
37 Cf. line 661 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.

6. Self-regulation – guidance and enforcement assistance

The principle of regulated self-regulation, which has proven itself at the national level in Germany, is not directly reflected in the guiding criteria, but there are points of reference in various places in the draft guidelines that address typical areas of responsibility for self-regulatory bodies.[38] This means that recommendations and positions issued by self-regulatory bodies such as the USK, as the one-stop shop for the games industry[39] in the field of youth media protection, are gaining legal and practical relevance.[40] They support their members in implementing their duties to protect minors in a legally compliant and effective manner. With their expertise, they contribute to the development of recognized minimum standards. In doing so, they offer guidance to providers, create realistic expectations, and promote consistency and transparency in implementation. This role is also in line with the international understanding of cooperative, multi-stakeholder-based youth media protection, as called for by the United Nations, among others.[41] Against this background, cooperation with recognized self-regulatory bodies such as USK appears to be a reasonable and responsible means of fulfilling regulatory requirements under the DSA.

7. Unexploited potential and inconsistency

Although the Commission's draft guidelines provide an important framework for online platforms, they fall short of expectations in terms of consistency, practicality, and systematic approach. Despite their recommended supportive nature pursuant to Article 28(4) DSA, the multitude of requirements and "should" phrases in some cases give the impression of a de facto obligation to implement all of the aspects mentioned, which contradicts the central principle of proportionality. An example such as that provided in § 24a(2) of the German Youth Protection Act (JuSchG) would be preferable in the interests of legal clarity. In addition, contradictory statements make consistent application difficult, for example when "highest" standards are required, even though Article 28(1) DSA only prescribes a "high level." The repeatedly described standard using terms such as "easy to use," "intuitive," or "engaging" may also lead to even committed providers being accused of user unfriendliness. The guidelines provide little guidance on user-centered implementation or prioritization, so that the sheer number of measures could be criticized as impractical.

There is also a lack of clarity regarding key terms; for example, "medium risks" are not defined, which provides little guidance. In the area of risk assessment, there is also an inappropriate mixing of youth protection and consumer protection standards, for example when the age of majority is used as a trigger for AVS obligations in terms and conditions. A clear separation of the two areas of law should be maintained in accordance with their respective protective purposes in order to avoid further increasing the risk of divergent legal developments due to double regulation.

Missed potential is evident in the lack of consideration given to proven effective models of preventive, self-regulatory approaches. A particular example is the automated rating system of the International Age Rating Coalition (IARC), which emerged from a global cooperation of such institutions and has now been reviewed and recognized by the German government.[42] IARC also assigns age ratings in the area of user-generated games (e.g., Fortnite). Age ratings that take into account usage risks and precautionary measures in line with age ratings and provide additional information on the features contained in the game and the main reasons for the age rating significantly increase the level of protection and also contribute to the required transparency (see 8.4 of the draft guidelines). This is achieved simply through their awareness-raising effect and even more so in combination with technical filters such as parental controls. In Germany, this is carried out on the basis of the JuSchG and, in future, also of the JMStV by the USK.

Statements regarding technical age assurance and tools for guardians, such as parental controls, are particularly concerning. The focus therefore remains disproportionately on AVS and age estimation. For example, many measures in the draft are linked to information about the user's age. Above all, however, although alternatives to age assurance should formally be possible (see III. 2.), the most obvious alternative (parental controls) is virtually denied any protective effect, even though it has high protective potential, safeguards key aspects such as participation and parental privilege (Art. 6 GG) and forms the basis for many other measures. Without such tools, protective measures can hardly be designed in an age- and situation-appropriate manner. This is particularly clear from the recommendations on "default settings," whose effect can only be realized through parental controls. This apparent devaluation is particularly questionable given that, according to the wording of the guiding principles, particular importance is attached to the area of "default settings" ("providers … that use default settings to ensure a high level of privacy, safety, and security of minors on their service") and that they are thus apparently intended to represent an alternative to age assurance, even though they are objectively directly linked to "tools for guardians." In addition to the focus on AVS, the discrepancy with the characteristic "accessible to minors," which is central to the scope of application of Article 28(1) DSA, is not resolved in a comprehensible manner. Furthermore, an analysis of the relevant risk categories reveals that mandatory age assurance in the present context is also questionable in terms of its effectiveness and proportionality in achieving the central protection goals in the digital space. Behavioral risks depend less on the "biological" age of a user than on social interactions and the structural characteristics of the platforms. Simply knowing a user's age does not influence the specific behavior of minors. AVS do not prevent young users from disclosing personal information or from engaging in risky or excessive behavior in the digital space. It should also be noted that experience under German youth protection law with regard to uniform EU standards on the "digital identity wallet" shows that such an approach is likely to be difficult to implement in practice.

IV. Conclusion

The draft guidelines contain numerous good approaches and specific provisions, but their structure, coherence, and practical feasibility fall short of the requirements for a rigorous and realistic regulatory framework. For the effective implementation of Article 28(1) DSA, further clarification, prioritization, and integration with existing instruments-including at the national level-are necessary. Particularly with regard to age assurance, the system and interlocking nature of the measures and the overall ob-

38 Cf. in particular lines 908 et seq. ("Governance") and 953 et seq. ("Monitoring and evaluation"), but also lines 635 et seq. and 714 et seq. of the draft guidelines pursuant to Art. 28(4) of the EU Commission of May 13, 2025.

39 Hentsch/von Petersdorff MMR Supplement 8/2020, 3 et seq.

40 Cf. Müller-Terpitz/Köhler/Holznagel, 2024, DSA Art. 28 Rn. 21–23; likewise Mast/Kettemann/Dreyer/Schulz, 2024, DSA Art. 28 mn. 71 et seq., which emphasizes processes and procedures in the target dimension "protection" and mentions cooperation with external experts in the protection of children and young people in the media, the appointment of a child and youth protection officer (beyond § 7 JMStV) or cooperation with external advisory and/or complaints bodies.

41 Cf. UN Committee on the Rights of the Child, General Comment No. 25 (2021), Section V, "C. Coordination," No. 27.

42 Cf. USK press release dated April 25, 2025, available at: https://usk.de/starker-digitaler-kinder-und-jugendschutz-automatisiertes-system-der-usk-fuer-altersken nzeichen-auf-online-spieleplattformen-ueberzeugt-jugendschutzbehoerden-der-bundeslaender/.

jective of the guidelines remain unclear. All that remains is the assumption that age assurance will in future serve as a means of "setting the course" " for the accessibility of the respective functions and content on online platforms. However, in view of the application criterion of online platforms being "accessible to minors," such systems cannot be intended to establish blanket access barriers for closed user groups within the meaning of the JMStV.

Lorenzo von Petersdorff
is deputy managing director and legal counsel of Unterhaltungssoftware Selbstkontrolle (USK), head of the USK.online division, and deputy member of the advisory board of the Digital Game Culture Foundation.

Quick read ...

- Art. 28 DSA establishes protection standards for minors on online platforms for the first time.
- The EU Commission's draft guidelines fall short of expectations in terms of structure, coherence, and feasibility.
- The strong focus on technical age verification misses out on potential for potential in terms of proportionate and proven (self-regulatory) approaches such as parental controls and age ratings.
- Unclear terms and contradictory standards make it difficult for platform providers to apply the guidelines in a legally compliant manner.

PATRICK MITSCHING / CHRISTIAN RAUDA

Content moderation in online games under the DSA

Initial experiences with implementing the transparency obligations under Articles 14 to 17 DSA

Reporting and remedy procedure

The Digital Services Act (DSA) expands the regulation of online games by imposing new transparency obligations for content moderation. Although online game providers have always had tiered moderation systems in place, these are now becoming more uniform and strictly regulated. Providers must make restrictions on user-generated content even simpler, clearer, and more understandable, especially for underage players. They must also publish annual transparency reports on notifications and corrective measures relating to content. Finally, corrective decisions must now be justified in greater detail and specific complaint procedures must be provided. This article highlights how the well-intentioned regulations currently ensure one thing above all else: more organizational effort for providers without clear improvements for users. In particular, it highlights the challenges of formulating content restrictions, preparing transparency reports, and changing remedial and complaint procedures. reading time: 20 minutes

I. Introduction

With the entry into force of the Digital Services Act (DSA), a significant change is taking place in the regulatory landscape for online games with multiplayer modes. Providers of such games are mostly classified as hosting services, as they allow players to share their own content, such as voice and text chat, images, screenshots, videos, etc., with other players. This sharing of content is a secondary function of playing together. It serves primarily to coordinate the completion of joint tasks within the game itself. However, it sometimes extends to social interaction outside the game in associated chat rooms, forums, instant messengers, etc., provided that these are made available by the game provider as a supplement to the game. Large amounts of user-generated content are generated both within and outside the game. Game providers have always had tiered penalty systems in place to deal with such content, but the DSA now takes this to a whole new level.

Since the DSA came into force, game providers have had to comply with new transparency obligations regarding content moderation under Articles 14 to 17 of the DSA. Content moderation refers to the procedures and organized practices for reviewing user-generated content published on hosting services to determine whether it complies with the provider's terms and conditions and public law.[1] Public law in Germany consists primarily of the DSA, the EU Regulation on addressing the dissemination of terrorist content online, the Criminal Code, the Youth Protection Act, and the State Treaty on the Protection of Minors in the Media. Game providers employ moderators who carry out content moderation on their behalf or as their representatives. Game providers have an interest in effective content moderation, as it increases the attractiveness of their games and reduces the risk of liability for legal violations. This article describes initial experiences with the implementation of the transparency obligations under Articles 14 to 17 DSA by game providers.

II. Restrictions on user-generated content in the terms and conditions

Terms and conditions play an important role for game providers. On the one hand, the terms and conditions establish the contractual legal framework between the user of the game and the

1 BNetzA, Status quo of specific measures taken by hosting services for content moderation, 2024, available at: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Internet/TerrorOnlIn/Studie.pdf.

game provider. However, they also have an important factual regulatory effect between users. Since users interact with each other in online games with multiplayer mode, it is crucial for them that their fellow players also adhere to the rules set by the game provider. After all, in the absence of contractual relationships, there are no direct claims between users. Users therefore frequently complain to game providers about violations by other users.

The establishment of rules for user-generated content is very important because it has a significant impact on the atmosphere of communication between users. This affects the "interaction" between users of a game, whose appeal lies in particular in its multiplayer mode. The degree of regulation by the game provider is an important factor for some players when choosing which games to play. Some players appreciate it, for example, when forums do not allow other players to be addressed in a manner that is rude but clearly below the threshold of criminal liability. For example, there are different approaches to whether it is permissible to call another user a "noob." "Noob" is not a swear word per se, but a term used to describe an inexperienced player. Nevertheless, the term is slightly derogatory. The term is derived from the English word "newbie," which means "beginner." A noob is characterized by a lack of experience, which manifests itself in clumsy moves.

Art. 14 (1) sentence 1 DSA stipulates that, in addition to restrictions on user-generated content, game providers must also provide information "on all guidelines, procedures, measures, and tools used to moderate content, including algorithmic decision-making and human review, as well as the procedural rules for their internal complaint management system." The purpose of this provision is to ensure that users are made aware, when concluding their contract with the game provider, of the rules that apply when the game provider checks whether user-generated content complies with the rules set out in the terms and conditions. The term "content moderation" is defined at length in Art. 3 lit. t DSA. According to this, it refers to "the activities, whether automated or not, of providers of intermediary services, which are intended to identify, detect, and combat, in particular, illegal content or information provided by users that is incompatible with the provider's terms and conditions, including measures relating to the availability, display, and accessibility of the illegal content or information, such as downgrading, demonetization, blocking access, or removal, or in relation to the ability of users to provide such information, such as closing or suspending a user's account."

Typically, providers of games with multiplayer modes have been using a tiered penalty system for many years-long before the DSA came into force. Although the design of this system varies from game provider to game provider, similarities have emerged over time. The lowest threshold for intervention is the removal of content, as this only means that the user's content is no longer accessible, but the users themselves are not subject to any measures that restrict them in the future. The next level of escalation is to restrict the player's ability to use aspects of the game, for example by disabling the chat function, revoking the right to post forum contributions, and deactivating the voice chat function (if the game offers such a function). These measures are intended to ensure that no further violations occur in the future without depriving the user of the opportunity to play the game. The third escalation level consists of temporarily but completely blocking access to the game. Such a temporary freezing of access is referred to in the gaming industry as a "suspension." This means that players will not be able to use the game for a certain period of time. After this period, however, the player will be granted access again. The highest escalation level consists of permanently blocking access to the game (known as a "ban" in the gaming industry).

Art. 14 (1) sentence 2 DSA stipulates that the information specified in Art. 14 (1) sentence 1 DSA must be written in clear, simple, understandable, user-friendly, and unambiguous language and made publicly available in an easily accessible and machine-readable form. Players should therefore be able to easily understand the rules and procedures of the game provider for moderating content. Game providers face the challenge of presenting the rules in a sufficiently concrete manner, as highly abstract rules are more difficult to understand. However, it should be noted that overly specific provisions run the risk of failing to anticipate certain cases that remain unregulated. Game providers are therefore advised to include lists of examples of unacceptable content in their terms of use and to update these lists regularly if behaviors occur that were not covered but are to be sanctioned in the future.

Typical unacceptable behaviors prohibited in terms and conditions include violations of personal rights, copyright infringements, and the distribution of pornographic, violent, sexist, right-wing extremist, or left-wing extremist content.

III. Communication of restrictions to underage players

In addition to the general restrictions for intermediary services specified in the DSA, the Digital Services Act (DSA) also contains explicit provisions designed to ensure the protection of children and teenagers.[2] The EU legislator's intention to provide greater protection for minors in the online environment is expressed, among other things, in Art. 14(3) DSA.[3] According to this, providers of intermediary services that are "primarily" aimed at minors or predominantly used by them have special obligations regarding the comprehensibility of their terms of use.

1. Target group: "Primarily" aimed at minors

The DSA leaves open the question of what constitutes "predominant" use by minors.[4] The decisive factor is either the objective focus of the intermediary service or the number of minor users.[5] The focus can be determined, for example, by the design or marketing of the service. A simple majority of over 50% is sufficient to assume predominant use by minors. [6]

Due to their colorful graphics, many games give the impression that they are mainly played by children, while the actual user base often consists of people over 30 years of age and sometimes even significantly older. It is therefore important to examine each case individually.

In the games industry, most providers of multiplayer online games exclude users under the age of 16 (in some cases even users under the age of 18) in their terms and conditions.

2. Requirements for the wording

If minors, i.e., persons under the age of 16, are permitted, the terms and conditions must be presented in an understandable form to ensure that they can be read and understood in all cases.[7] The DSA leaves open exactly what the requirements for youth-appropriate wording should be.[8]

2 BzKJAKTUELL 1/2024, 8, (11).
3 Recital 46 DSA; Barudi, in: Müller-Terpitz/Köhler, DSA, 2024, Art. 14 Rn. 22.
4 Barudi, in: Müller-Terpitz/Köhler, DSA, 2024, Art. 14 Rn. 22.
5 Recital 46 DSA.
6 Hofmann/Raue, DSA, DSA, 2023 Art. 14 Rn. 70.
7 Barudi, in: Müller-Terpitz/Köhler, DSA/, 2024, Art. 14 Rn. 22.
8 Barudi, in: Müller-Terpitz/Köhler, DSA/, 2024, Art. 14 Rn. 22.

The texts must be formulated in such a way that minors can understand them, i.e., in a manner appropriate for children and young people. A similar wording can be found in Section 24a (2) sentence 8 JuSchG, according to which "the provisions of the general terms and conditions that are essential for use must be presented in a child-friendly manner." However, even a more comprehensible version of the terms of use does not alter the assumption that children and teenagers would not read these terms and conditions in most cases. [9]

3. Requirements for content

However, establishing "double terms and conditions," i.e., special "youth terms and conditions" in addition to the conventional terms and conditions, would place minors at an undue disadvantage.[10] Consequently, "youth-friendly terms and conditions" within the meaning of Art. 14 (3) DSA are not terms and conditions at all, but merely explanatory information that accompanies the applicable terms and conditions at .[11] This is also supported by the wording of Art. 14 (3) DSA, which refers to an explanation of the provisions and not, for example, to the drafting of separate terms and conditions.[12]

The wording in Art. 14 para. 3 DSA, according to which "conditions and any restrictions on the use of the service" must be explained, obliges the intermediary service to prepare and make available the entire terms and conditions in a manner appropriate for minors.[13] In this respect, the DSA is more precise than the JuSchG, which in Section 24a merely requires the "essential provisions" to be presented. In particular, those provisions of the terms and conditions that deal with the main obligations and the processing of personal data should be clearly transposed.[14]

According to the wording of Art. 14 (3) DSA, rules included in the terms and conditions, such as community guidelines, must also be prepared in a youth-friendly manner insofar as they refer to "conditions and any restrictions."[15] However, the specific requirements for explanations in youth-friendly language have not been specified by the legislator and therefore offer relatively broad scope for interpretation.[16] Providers could, for example, use audiovisual representations of the content to be explained, explanatory videos, pictograms, or similar.[17] This could also solve the above-mentioned problem that texts may not be read by children and teenagers. In addition, the explanations should also be available in the various native languages of the user groups.[18]

4. Communication with minors

With regard to data processing by game providers, Article 8(1) sentence 1 of the GDPR stipulates that minors aged 16 and over may consent to data processing themselves, provided that this is done expressly and voluntarily and that the minor has been adequately informed (in a manner appropriate to their age) about the specific data processing and their rights. Younger users of games must either obtain the consent of their legal representatives to their own consent or provide direct consent from their legal guardians in order to consent to data processing. Age can be queried and verified using parental control systems in order to comply with the protection of minors and Art. 8 (2) GDPR if the minor is under 16 years of age.[19] Large game providers such as Epic, Nintendo, and Roblox have sophisticated systems in place for this purpose.

IV. Transparency reporting obligations

1. New requirements and status of implementation

The annual transparency reports to be prepared in accordance with Art. 15 DSA represent a new challenge for online game providers. It should be noted that such reports have so far only been published by a few large providers.[20] In contrast, there are hardly any reports from medium-sized providers,[21] although the majority of them are likely to be covered by Art. 15 DSA as hosting service providers. Even though small and micro-enterprises with fewer than 50 employees and less than EUR 10 million in annual turnover are exempt from the reporting obligation under Article 15(2) DSA, an estimated 30-40 game providers based in Germany are likely to remain subject to the reporting obligation.[22] The fact that there have been hardly any transparency reports from SMEs to date may be due, on the one hand, to a lack of information about the existence of the legal obligation and, on the other hand, to the very high cost of preparing the reports. As an example, it should be noted that InnoGames GmbH, a medium-sized provider, required approximately 100 person-hours to prepare its 2024 transparency report.

2. Form of the reports

The transparency reports published by game providers for the first reporting year 2024 still differed significantly in form: Some providers published elaborately laid-out reports with lengthy explanations, while others provided simple sheets with tables that were more or less uncommented.[23] Some providers' reports were two A4 pages long, while others were 38 A4 pages long – even among providers of comparable size.[24] Starting with the reporting year 2025, the EU Commission now wants to put an end to this "Wild West" with an implementing regulation pursuant to Art. 15 (3) DSA.[25] Starting in July 2025, all providers must use standardized reporting forms. Unlike very large online platforms (VLOPs) and very large online search engines (VLOEs), which are required to report every six months, this will affect game providers for the first time on the submission date for the 2025 calendar year, February 28, 2026. The

9 Dregelies MMR 2022, 1033 (1036).
10 Liesching, Jugendschutzrecht (Youth Protection Law), 6th edition 2022, § 24a margin note 67.
11 Hofmann/Raue, DSA, 2023, Art. 14 Rn. 71.
12 Hofmann/Raue, DSA, 2023 Art. 14 margin note 71
13 FSM, Youth-friendly terms and conditions – The legal interpretation of Art. 14 (3) DSA, p. 2, available at: https://www.jff.de/fileadmin/user_upload/jff/projekte/Jugendgerechte_AGB/Jugend-AGB_Rechtliche_Interpretation_DSA.pdf.
14 Erdemir/Bernzen/Dreyer, JuSchG, 2024 § 5 Rn. 89.
15 FSM, Youth-friendly terms and conditions – The legal interpretation of Art. 14 (3) DSA, p. 3, available at: https://www.jff.de/fileadmin/user_upload/jff/projekte/Jugendgerechte_AGB/Jugend-AGB_Rechtliche_Interpretation_DSA.pdf.
16 BzKJAKTUELL 1/2024, 24 (25).
17 Liesching, Jugendschutzrecht (Youth Protection Law), 6th edition 2022, Section 24a, margin number 66.
18 Erdemir/Bernzen/Dreyer, JuSchG, 2024 § 5 margin note 91.
19 Bänsch/Hentsch MMR Supplement 8/2021, 3 (6).
20 Electronic Arts, available at: https://media.contentapi.ea.com/content/dam/ea/com/common/transparency-report-2024.pdf; Nintendo, available at: https://www.nintendo.com/eu/media/downloads/legal_1/DSA_Transparency_Report_as_at_28th_February_2025.pdf; Square Enix, available at: https://static.square-enix-games.com/Square_Enix_ DSA_Transparency_Report.pdf; Take-Two Interactive, available at: https://ir.take2games.com/static-files/b7784109-bccb-48df-83f6-e76bdd37b2af; XBox, available at: https://www.xbox.com/en-US/legal/xbox-transparency-report.
21 InnoGames: tbd; Wooga, available at: https://www.wooga.com/legal/eu-digital-services-act-information-en.
22 GamesWirtschaft, The largest game studios in Germany in 2024, available at: https://www.gameswirtschaft.de/wirtschaft/groesste-games-studios-deutschland-2024-150824/.
23 Electronic Arts, Take-Two Interactive: layout text, Wooga: Excel spreadsheet.
24 Nintendo: 2 pages, Xbox: 38 pages.
25 EU Commission, Commission harmonizes rules on transparency reporting under the Digital Services Act, available at: https://digital-strategy.ec.europa.eu/de/news/commission-harmonises-transparency-reporting-rules-under-digital-services-act.

reporting forms are available as CSV and XLSX spreadsheet templates on the Commission's website and are accompanied by a 32-page instruction manual.[26]

3. Criticism of formal requirements

Despite all the understandable efforts to achieve uniformity and comparability, the new reporting form is a bureaucratic nightmare: there is only one template for all types of providers, regardless of whether they are a simple intermediary service or a very large online platform or search engine. As a result, each form consists of 11 spreadsheets, the largest of which are 180 lines long and 20 columns wide. Game providers must first delete all cells that are not applicable to them. Then they have to enter figures page by page into the unwieldy spreadsheet templates. To make matters worse, the instructions for completing the form are only available in English on the Commission's website. The new reporting form has made the process very cumbersome. In fact, it can only be handled by specialized compliance and legal departments, which many medium-sized game providers do not have. This raises the question of why the Commission has opted for huge and cumbersome Excel spreadsheets as the mandatory reporting format. It would be more effective if there were a standard online form for all providers that only requested the relevant reporting information depending on the type of provider.

4. Content of the reports

In terms of content, the transparency reports published in 2024 also reveal a wide variety. The core of the reports is the information on orders from member states and reports from individuals and entities pursuant to Art. 15 (1) (a) and (b) DSA. Here, providers must break down the number of orders and reports received according to the type of allegedly illegal content concerned. It is interesting to note how differently game providers have categorized the types of content: Most providers have categories for

- threats and violence,
- harassment and stalking,
- fraud,
- hate speech and
- sexual content.

In contrast, only a few providers, list

- cheating,
- data misuse,
- malware and phishing,
- public safety and terrorism, or
- spam and unauthorized advertising

separately. It can be assumed that the latter types of content have not been recorded separately by providers to date, or have only been listed as "Other." Overall, most providers specify between 5 and 10 categories.

Here, too, the EU Commission is now intervening with standardized reporting forms. These specify the categories of illegal content in detail. There are a total of 15 main categories, each with up to 7 subcategories, for a total of 99 parameters. These range from main category 1, "Animal welfare," to main category 15, "Other violations of the provider's terms and conditions." To illustrate the level of detail in the subcategories, category 3, "Cyber violence," is given here as an example: This contains the subcategories 3a "Bullying and intimidation," 3b "Cyber harassment," 3c "Incitement to violence or hatred," 3d "Cyberstalking," 3e "Non-consensual sharing of intimate material," 3f "Non-consensual sharing of material edited using deepfake technology," and 3g "Other." The main and subcategories are so detailed that the transparency reports resemble the data collection forms used in long-term scientific studies.

5. Criticism of content guidelines

This extreme level of detail presents game providers with the challenge of converting their existing internal categorization to this new quasi-EU standard. This is a huge task, as most existing reporting systems are much simpler in design. This is clearly evident from the transparency reports published in 2024, in which most providers only list 5 to 10 main categories and no subcategories. In fact, certain categories do not even exist among game providers: for example, pyramid schemes, animal cruelty, and environmental hazards are very rare in the gaming context, but must still be included in the reporting forms. It is also sometimes difficult to select the right category: for example, when a distinction must be made between category 3 "cyber violence" and category 4 "cyber violence against women," even though game providers do not regularly record the gender of players due to lack of relevance and data minimization. Or when a distinction must be made between subcategories 3a "cyberbullying," 3b "cyberharassment," and 3c "cyberstalking," even though the facts are often vague and fit several subcategories.

In addition, the categories in the reporting form differ from those in other countries, creating a divergence problem. For example, the 99 parameters of the DSA are inconsistent with the 130 priority offenses of the UK Online Safety Act.[27] However, most game providers are economically active in both the EU and the UK. In practice, this means that all reports must be recorded in parallel in both category systems for the EU and the UK, which entails considerable additional work. This does not even take into account other countries outside the EU that intend to enact their own laws on online harms in the future. It would be desirable for such requirements to be harmonized within Europe and the OECD.

Another, more legal challenge for game providers is the differentiation according to the legal basis under Art. 15(1)(b)(3) DSA. According to this, providers must differentiate for each measure taken as a result of a report whether it was taken on the basis of general laws or their own terms and conditions. In practice, this is often difficult to distinguish because the terms and conditions usually reflect the public law of the provider's country of residence. In Germany, for example, cyberstalking is now regulated in Section 283 of the Criminal Code, but is also prohibited under the terms and conditions of most game providers. It is therefore impossible to say whether a measure against cyberstalking was taken on the basis of general laws or the provider's own terms and conditions, because both apply.

V. Establishment of reporting and remedy procedures

1. New requirements and status of implementation

Providers of online games have always had reporting and remedy procedures in place for user-generated content. What is new about the reporting procedure provided for in Art. 16 DSA is that reporters must provide more of their own personal data and submit a declaration of accuracy and completeness. Art. 16 (2) (c) DSA requires the name and email address of the person or entity making the report to be provided. Article 16(2)(d) DSA also

26 EU Commission, Implementing Regulation laying down templates for transparency reporting obligations of online platform providers, available at: https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations.

27 OFCOM, Overview of Illegal Harms, available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/overview-of-illegal-harms.pdf?v=390985.

requires a statement that the reporting party is convinced in good faith that the report is accurate and complete. This is unusual for the gaming industry, as players usually use a pseudonym instead of their real name. In addition, when registering for an online game, players are increasingly reluctant to disclose their email address to the game provider: Login is increasingly taking place via third-party platforms such as Apple (App Store), Google (Play Store), Microsoft (Xbox), Nintendo (Switch Online), Sony (Playstation), and Valve (Steam), whereby the email address is not passed on to the actual game provider. It is also unusual to provide a comprehensive legal declaration of accuracy and completeness when registering – an informal notification has usually been sufficient up to now.

In addition, pursuant to Art. 17 DSA, game providers must now provide more detailed reasons for their remedial decisions. They are required to provide "clear and specific reasons" for all restrictions. Pursuant to Art. 17(3)(a) DSA, these reasons must include the facts and circumstances on which the decision is based. In addition, pursuant to Art. 17(3)(b) DSA, it must indicate whether the decision was based on a report by a user or on voluntary investigation by the game provider on its own initiative and, in certain cases, even the identity of the reporting person. Although moderation decisions in online games are already justified, this is often only done briefly and concisely. Art. 17 DSA, on the other hand, seems to require a full "statement of facts" as in court judgments. Another particularly critical aspect for game providers is that they must indicate whether the decision was based on a user report or their own investigation. Providers often deliberately remain vague in this regard in order to protect their sources of information. This is particularly problematic in cases of cheating, which now falls under the DSA as a miscellaneous violation of the provider's terms and conditions.

2. Criticism of the requirements

The new requirements regarding real names, address details, and declarations of accuracy and completeness for content reports represent a break with the successful informal reporting culture in the online gaming sector. For players, they are a step backward from the status quo, as they make anonymous and suspicion-based reports difficult or impossible and expose those reporting to the risk of retaliation by those reported. This may have a chilling effect and even reduce the number of reports. Conversely, the requirement to justify remedial measures leads to unnecessary additional work. Worse still, this gives cheaters an opportunity to fish for information, as they can deduce the investigative path and possibly even the informants from the remedial decisions issued against them. It would be better to provide for exceptions to the obligation to provide reasons if this makes it more difficult for the game provider to detect future violations or take legal action.

VI. Conclusion

The obligations of game providers for content moderation resulting from the DSA entail considerable personnel, financial, and organizational costs. There was no need for regulation in the games industry, as almost all game providers have for many years, in their own interest and in the interest of the smooth use of games, maintained extensive technical systems and community management departments that ensure that users do not disseminate undesirable or dangerous content without consequences. From the players' point of view, it is to be welcomed that the sanctions for possible violations must be clearly defined in the terms of use.

The reporting requirements entail considerable expenditure and personnel resources for companies. The effect of such transparency reports – if they are read at all – is minimal. While there are currently calls across all political camps for a reduction in bureaucracy, EU regulation is constantly creating new bureaucratic obligations. The additional requirements for reporting and remedial procedures are also counterproductive. The reporting procedures contradict the data protection principle of data minimization. In addition, helpful anonymous and suspicion-based reports are made more difficult. The corrective measures create an unnecessarily high burden of proof. On the other hand, new opportunities to fish for information arise for cheaters.

Overall, the implementation effort resulting from the DSA is considerable. However, the situation for users will hardly improve compared to the de facto status quo before the DSA came into force. The positive effects of the DSA should be evaluated after a few years to decide whether to remove bureaucratic hurdles if the desired effect of the regulation has not been achieved.

Quick read ...

- Game providers must comply with the transparency obligations under Articles 14 to 17 DSA when moderating content. Content moderation refers to the procedures for reviewing user-generated content for compliance with terms and conditions and public law.
- Typically, providers of games with multiplayer mode rely on a tiered system of sanctions: removal of content, restriction of use, temporary suspension, and finally permanent exclusion.
- If persons under the age of 16 are permitted, the terms and conditions must be presented in an easy-to-understand form.
- The requirements for transparency reports are a bureaucratic nightmare.
- In addition to regulations on reporting and remedy procedures, the new requirements regarding real names, address details, and declarations of accuracy and completeness represent a break with the successful informal reporting culture in the online gaming sector.

Patrick Mitsching, LL.M. (Durham), M.A. (London),
is head of the legal department at InnoGames GmbH in Hamburg.

Professor Dr. Christian Rauda
is a specialist lawyer for IT law, copyright and media law, industrial property rights, and a partner at the law firm ARTANA in Hamburg, as well as a professor of computer game law and entrepreneurship in the games industry at HTW Berlin.

OLAF WOLTERS

New compliance requirements for a secure digital ecosystem

Recommendations for game developers and platform operators

Compliance management system

The Digital Services Act (DSA) marks a fundamental change in the regulation of digital services and, in particular, presents the gaming industry with new compliance management requirements. With its differentiated regulatory approach – ranging from pure conduit services to online platforms and search engines – the DSA aims to create a secure digital ecosystem and effectively curb illegal content. Fortunately, in practice, it is clear that key elements of the DSA requirements have already been largely anticipated and implemented by leading platform providers and online game operators. These include internal processes and guidelines, reporting and complaint mechanisms, extensive transparency obligations and specific obligations for very large online platforms.

reading time: 22 minutes

I. Introduction

The Digital Services Act (DSA) pursues a graduated regulatory approach depending on the function and size of the service provider. According to Article 3 DSA, pure conduit services, caching services, hosting services, online platforms and online search engines are covered. In the gaming sector, these include platforms such as Steam, Origin, Playstation Network, Xbox Gaming, Nintendo eShop, Epic Store, but also communication platforms such as Discord and TeamSpeak.

The European legislator has expressly recognised the relevance of the DSA for computer and video games and, in its resolution on the internal market concept for consumer protection in online video games of 18 January 2023, called for the creation of a safe digital environment and the rapid application of the DSA with regard to the dissemination of illegal content via in-game communication functions[1] .

One of the most important requirements of the DSA is the maintenance of a compliance management system (CMS). In the games industry, which is dominated by small and medium-sized enterprises, the issue of compliance is, as is generally the case in SMEs, rather underdeveloped. Against this background, it is worth taking a look at the most important aspects of the DSA with regard to compliance.

II. Principles of DSA compliance management

First, it is worth taking a look at the general structure of compliance management systems (CMS)[2] . This includes defining rules and processes, introducing an organisational structure, training and raising awareness among employees, and finally monitoring and continuously improving the CMS.

1. Implementation of internal processes and guidelines

To implement the requirements of the DSA, digital service providers should first implement internal processes and guidelines. These serve to effectively moderate content, ensure transparency and enable legally compliant communication with users and authorities[3] .

Another important requirement for the service providers covered is the establishment of a reporting and redress procedure for the removal of illegal content in accordance with Art. 16 DSA. This includes the creation of transparent and easily understandable guidelines that define what content is considered illegal and under what conditions it will be removed or blocked. Moderation should be based on applicable EU law and national regulations, particularly in areas such as hate speech, terrorist propaganda and copyright infringements. To ensure efficient implementation, standardised review procedures must be introduced to identify, assess and remove illegal content. This requires both training for moderation teams and the use of automated systems to ensure fast and accurate processing[4] .

This should not pose any major challenges for game providers. Community guidelines and rules of play, including anti-cheat policies, are common standards, especially for online multiplayer games.

Another key point is the establishment of a complaint mechanism for users in accordance with Art. 20 DSA. Platforms must provide a user-friendly reporting procedure that allows users to report illegal content. It is essential that these reports are processed quickly and transparently by a trained moderation team[5] . In addition, a complaint mechanism must be set up through which affected users can appeal decisions to remove or restrict their content. Transparency plays an important role here: users must be informed about decisions made, the reasons for them and possible avenues of appeal. In certain cases, an external dispute resolution procedure may be offered to enable independent review of moderation decisions[6] .

Here, too, at least the technical requirements should not pose any major hurdles for game providers. The games industry is a pioneer in target group communication via the Internet. Since the triumph of online games in the mid-2000s and the online capability of the most important gaming platforms, providers and players have been in direct contact via user accounts in order to process complaints and support requests directly.

To ensure traceability and compliance with the DSA requirements, service providers have specific transparency reporting obligations and associated documentation and reporting procedures in accordance with Articles 15 and 42 of the DSA. This inh

1 European Parliament resolution on the internal market approach to consumer protection in online video games (2022/2014 (INI)), paragraph 46.
2 For details on compliance structures, see Goette/Barring DStR 2021, 1238 ff.
3 See recital 5 of the DSA.
4 See Mitsching/Rauda MMR 2025, 674 – in this issue.
5 See Recital 58 DSA.
6 Recital 149 DSA explicitly mentions class actions and consumer protection associations.

cludes the introduction of a standardised documentation process for recording all moderation decisions. The information recorded includes the number and type of reported content, decisions on whether to remove or retain content, the results of complaints and the use of automated systems for content moderation. Companies are required to produce regular transparency reports that are made publicly available and demonstrate compliance with the DSA requirements. In addition, there is close cooperation with supervisory authorities and digital service coordinators (DSCs) to ensure legally compliant reporting.

Small and micro-enterprises are exempt from this obligation under Article 19 of the DSA. According to the EU Commission Recommendation (2003/361/EC) concerning the definition of micro, small and medium-sized enterprises (EU SME definition), an enterprise is an SME if it employs fewer than 250 persons and has an annual turnover not exceeding EUR 50 million or an annual balance sheet total not exceeding EUR 43 million. This is likely to include approximately 99% of companies operating on the German market.

Nevertheless, these companies should also maintain a complaint management system in light of the Whistleblower Protection Act (HinSchG), as the HinSchG requires a whistleblower system for companies with 50 or more employees.

2. Compliance organisation

Every functioning CMS also provides for the sensible design of a compliance organisation. There is no legally prescribed or customary structure that must be implemented. Since compliance is influenced by numerous factors, the organisation, measures and control systems should be adapted to the company and take its specific needs into account[7] .

In practice, the tasks will be performed either by a newly created compliance function or by a specifically appointed officer within existing structures[8] . The compliance function should report directly to senior management and be responsible for ensuring and monitoring DSA compliance . It will also ensure effective cooperation between different departments, e.g. the legal department, which will be responsible for implementing the legal obligations under the DSA, in particular reporting and due diligence obligations at the governance level, the IT department, which will be responsible for implementing mechanisms for algorithm transparency and risk assessments, the content moderation function, which will ensure fair and objective moderation decisions in accordance with the requirements of Art. 16 to 20 of the DSA, and finally, the data protection officer should be involved, who should coordinate with data protection requirements in connection with the GDPR.

Companies in the games industry are experienced in regulation. In addition to youth protection requirements, there are also numerous consumer protection implications for games, so it makes sense to link the compliance function to existing structures.

However, Article 41 DSA imposes special requirements on the compliance organisation of very large online platforms (VLOPs) and very large online search engines (VLOSEs). These companies must establish an explicitly independent compliance function to ensure compliance with the legal requirements. Platforms with more than 45 million monthly active users in the EU are considered VLOPs. So far, the EU has not classified any gaming platforms as VLOPs. Against this background, the independence of the compliance function is likely to require a structure outside the normal reporting line.

However, very few companies in the gaming industry are likely to be classified as VLOPs. The PlayStation Network (PSN) will have a total of 129 million monthly active users worldwide by the end of 2024. Depending on the EU's share of the total market, the 45 million user mark is likely to be reached soon. Similar user numbers are expected for Microsoft's Xbox Gaming.

3. Training and awareness

In addition to adequate compliance organisation, another important component of any CMS is a training and education programme.[9] The DSA takes this into account and provides for ongoing training of employees to raise their awareness of the regulatory requirements[10] . Articles 15 and 42 of the DSA even require that employee training measures be included in the transparency report.

Particularly in the area of content moderation and the technical implementation of the DSA, in-depth knowledge of legal requirements and the respective platform guidelines is essential. Companies should therefore establish ongoing training programmes to ensure that their teams have the necessary skills to correctly apply the moderation guidelines and implement legal obligations. This training should be practical and cover both the identification and removal of illegal content and the complaint procedure itself in accordance with the requirements of the DSA. This is likely to be in addition to the content-related issues.

In the gaming sector, the boundaries between support and content moderation are likely to be fluid. In particular, games with integrated chat functions, such as most first-person shooters, often already have complaint mechanisms in place to suppress flaming, cheating or the use of illegal symbols. In addition, technical systems are already used in online games to detect and block illegal user-generated content and fraud software.

In addition to technical and legal aspects, training should also cover ethical issues, particularly with regard to the protection of freedom of expression and the responsible use of automated decision-making processes. Another focus is on raising awareness of algorithm transparency and the responsible use of AI-supported moderation, as required by Article 27 of the DSA[11] .

Employees should understand how algorithmic systems are used to detect, filter and moderate content and what potential risks are associated with this, particularly with regard to discrimination, misjudgement or lack of transparency. They should also be trained in how algorithmic decisions can be reviewed and, if necessary, corrected to ensure fair and legally compliant content moderation.

4. Continuous monitoring and improvement

Finally, effective compliance management requires continuous monitoring and improvement of existing structures and processes in order to identify and close any gaps[12] . A central component of this process is therefore the implementation of a control system that enables systematic monitoring and review of the compliance measures introduced. The guidelines and procedures for content moderation, transparency and user protection should be reviewed both automatically and manually. If deficiencies or quality issues are identified, these must be remedied and optimised immediately.

---

7 Kramer, IT-ArbR/Schulze/Zumkley, 3rd edition 2023, Section 2, marginal number 996,

8 Explanation on the structure of the compliance organisation Hoffmann/Schieffer NZG 2017, 404.

9 See on compliance training Kramer, IT-ArbR/Schulze/Zumkley, 3rd edition 2023, Section 2 marginal number 1066.

10 See recital 87 DSA.

11 Explanation in Recital 70 DSA.

12 Goette/Barring correctly refer to a "duty to subsequently reflect on the compliance management system", DStR 2021, 1240.

III. DSA compliance obligations by platform type in the games industry

The other specific compliance requirements of the DSA are also tiered and depend on the type and size of the digital services[13] .

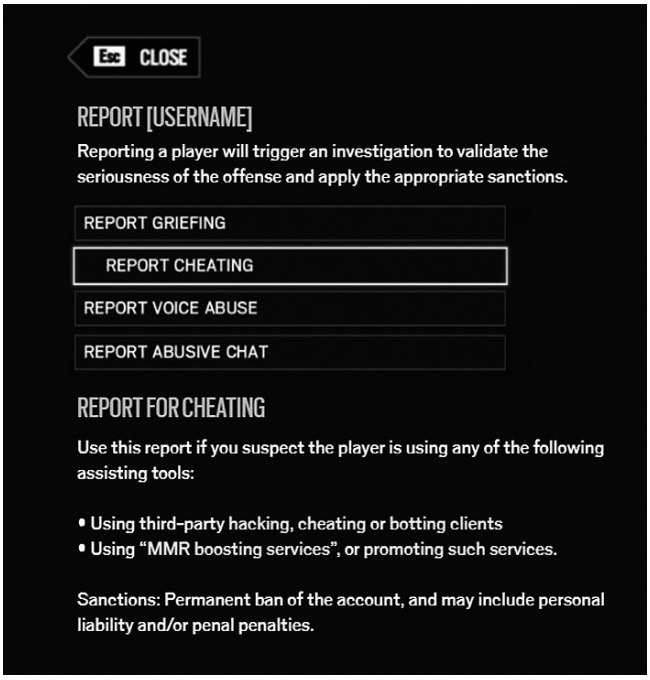
1. General obligations for all digital services

All digital services are subject to obligations that include, in particular, transparency and reporting requirements. For example, pursuant to Articles 11 and 12 of the DSA, all providers must establish an easily accessible point of contact for authorities and users through which legal inquiries and complaints can be submitted.

Providers that are not established in the Union are required under Article 13 DSA to appoint a legal representative. This is intended to facilitate communication and is particularly relevant for non-EU providers in terms of delivery and enforcement issues when dealing with authorities. The contact point should enable two-way communication and must therefore be more than a simple contact form[14] . An example of this would be a game developer who operates a multiplayer game and provides a support hotline or an online function through which users can report violations or security issues. This is already common practice and therefore does not pose a major challenge for providers.

The French provider Ubisoft, for example, maintains communication and complaint mechanisms both on its website[15] and directly implemented in many online games[16] . In the games themselves, it is possible to report "fellow players" live online, e.g. by selecting the "Show player" function and then selecting the default setting "Report player".

In Ubisoft's first-person shooter Rainbow Six Siege, the reporting window in the game looks like this, for example:



Source: Ubisoft

The procedure and consequences of reporting are described, and the reporting system also offers a selection of potential violations such as cheating or illegal chats. This makes reporting easier and motivates users to monitor compliance with the community rules themselves. At the same time, the guidelines should also meet the legal requirements described above.

In addition, companies are required under Article 15 DSA to publish an annual transparency report detailing, among other things, the moderation measures taken against illegal or inappropriate content. In the gaming industry, this could include the publication of statistics on user accounts blocked due to hate speech, fraud attempts or other violations within an online community.

Here, too, larger companies in particular are already active. Microsoft has been publishing an Xbox transparency report since 2022[17] . In this report, Microsoft provides comprehensive information about all activities related to the Xbox gaming platform and Xbox Game Studios games such as Age of Empires, Minecraft and Halo. Definitions, policies and guidelines are also linked[18] . The shared statistics are interesting, as they provide insight into the flood of data that needs to be moderated. According to the Transparency Report 2024, Microsoft moderated a total of 17.2 billion pieces of content between February and December 2024[19] . Microsoft includes text, user names, images and other user-generated content on its platforms in this content. According to the report, a total of 409 million pieces of content (2.4%) were classified as unacceptable. Of these, 209 million were classified as misuse of the platforms, 54 million pieces of content were classified as obscene and vulgar, 46 million as pornography, 32 million as bullying and harassment, and 27 million as hate speech. The content is monitored and recorded automatically. However, abuses were also reported. Microsoft received 53.2 million reports during the reporting period, which led to action in 9.2% of cases (5 million)[20] . Microsoft also relies on technology when it comes to the reports it receives and makes this transparent in the report: "At Xbox, we believe that automation and the use of AI-powered solutions such as Community Sift, combined with human expertise, play a critical and complementary role in effectively identifying, reporting and preventing harm at scale, especially as this online harm becomes increasingly sophisticated. Not only do they prevent unwanted content from reaching players, but they also reduce people's exposure to sensitive content and help focus human moderation on more nuanced and complex issues."

The statistics are impressive: during the reporting period, 1 million reports were reviewed manually and 4 million were processed automatically. A further 12 million pieces of content initially underwent an automated scan and were then checked manually. In total, the system recorded and analysed 400 million posts in a fully automated manner.

2. Additional requirements for hosting services and online platforms

Hosting services and online platforms are subject to additional requirements, particularly with regard to content moderation and complaint handling.

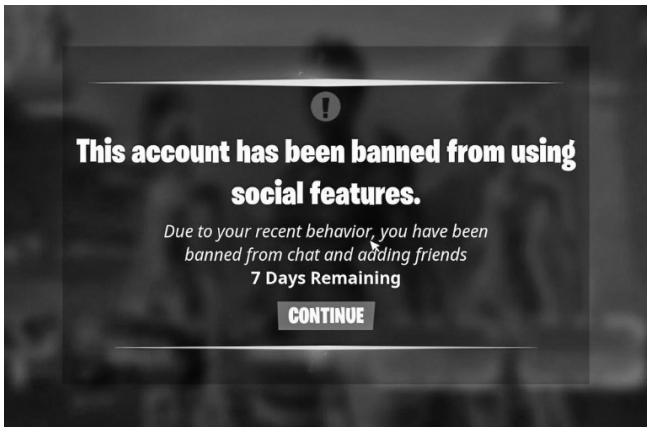
According to Article 16 of the DSA, providers must implement a user-friendly reporting system that allows users to report illegal content such as hate speech or copyright infringements. This means that there are now uniform requirements across Europe for a notice-and-takedown procedure to enable the electronic reporting of illegal content. It is regrettable that there is no internal conflict rule providing clarity on the applicable law. In Article 3(h) of the DSA, content is defined as illegal if it is "not in accordance with Union law or the law of a Member State".

13 See Kraul/Schmidt CCZ 2023, 177.
14 Recital 42 DSA.
15 Available at: https://www.ubisoft.com/de-de/help/contact.
16 Example available at: https://www.ubisoft.com/de-de/help/the-division-2/gameplay/article/blocking-players-in-the-division-2/000064952.
17 Transparency Report 2024, available at: https://www.xbox.com/de-DE/legal/xbox-transparency-report.
18 Available at: https://www.microsoft.com/en-ca/DigitalSafety/policies.
19 See page 20 of the Transparency Report 2024.
20 See page 22 of the Transparency Report 2024.

For the games industry, the status quo remains unchanged, e.g. with regard to anti-constitutional symbols or the protection of minors. Due to fragmented European regulation, e.g. in the area of youth protection, the industry has already established its own uniform European standards[21] and is therefore likely to welcome uniform European regulations.

In addition, Article 20 DSA requires an internal complaint mechanism that allows affected users to challenge moderation decisions. This could mean that a player whose account has been suspended for alleged violations would have the opportunity to appeal and request a review by a moderator. In this respect, too, online game providers already have established mechanisms in place, which are usually managed via the mandatory user accounts and can be accessed either within the games themselves or via the provider portal. The sanctions may be temporary or permanent.

Measures against abuse also play an important role. According to Art. 23 DSA, platforms must identify users and, if necessary, block them if they repeatedly violate platform guidelines or legal requirements. In the games industry, this is particularly relevant for online games with high moderation requirements, e.g. in titles such as "League of Legends" or "Call of Duty", where developers have established measures against cheating and toxic behaviour and implement them in practice.



Source: Epic Games

In addition, Article 30 DSA obliges platform operators to carry out a risk-based assessment of providers on online marketplaces. This applies, for example, to platforms such as the Steam Marketplace or the Epic Games Store, where third-party providers sell digital content. Here, providers would have to ensure that sellers do not distribute counterfeit or illegal content. Since most providers have already implemented extensive approval processes from a quality perspective, no new or increased requirements should arise from the DSA in this regard.

3. Strict requirements for very large online platforms

VLOPs are subject to particularly strict requirements because their reach means they potentially pose greater risks to society. For example, under Article 34 of the DSA, platforms must conduct an annual risk assessment to identify systemic risks such as the spread of disinformation or algorithmic bias. An example in the gaming industry would be a large platform such as Twitch, which must check whether its recommendation systems promote hate speech or extremist content. To mitigate risks, Article 35 DSA requires providers to develop targeted countermeasures, such as increased moderation or algorithm adjustments.

Another important aspect is the transparency of recommendation systems. According to Art. 27 DSA, platforms must disclose how their recommendation algorithms work. This applies, for example, to gaming platforms that display algorithmically generated game recommendations based on user behaviour. In addition, Article 38 DSA requires that alternative sorting options be provided so that users can choose between algorithmically sorted and chronological displays, for example. An example would be the implementation of a filter in digital game shops that allows users to sort games by release date or popularity, regardless of AI-based recommendations.

Finally, VLOPs are subject to increased external control. According to Art. 37 DSA, they are required to conduct independent annual audits to ensure compliance with DSA requirements. In the games industry, large platforms such as Xbox Live or Discord could also have their moderation practices independently audited. In addition, under Article 40 DSA, platform operators must provide authorised researchers with data for the purpose of investigating online risks. This could include, for example, the analysis of toxic player behaviour or algorithmically promoted disinformation in multiplayer games.

The DSA's tiered compliance requirements thus have a direct impact on the games industry. While smaller developers must meet basic transparency requirements, large gaming- platforms are subject to significantly greater regulation, particularly with regard to content moderation, algorithm transparency and abuse prevention. Consistent implementation of these requirements can help make digital gaming platforms safer, more transparent and fairer for all users.

IV. Practical implementation of a DSA compliance management system

The practical implementation of an effective DSA CMS requires a structured approach that includes both technical and organisational measures. A well-implemented CMS ensures that all DSA requirements regarding transparency, content moderation and risk management are met and should complement existing structures and processes. SMEs in particular should act with caution and avoid excessive effort.

The compliance structure and governance can be linked to existing structures. The legal department, human resources department and customer support are probably the best choice here. Smaller companies that outsource these functions, e.g. to a law firm or tax advisor, can use the solution for the requirements of the GDPR, which were also frequently outsourced, as a model.

Against this background, it makes sense to appoint a compliance officer. This person should regularly liaise with the relevant internal departments, such as the legal department, the product department and content moderation, as well as external consultants, to ensure that both legal requirements and best practices are observed.

Technical and organisational measures can also be linked to existing and established structures. The implementation of automated filter and moderation tools has long been standard in online games as a "profanity filter"[22] . These tools are now equipped with AI and machine learning to automatically identify problematic content and block it immediately. As a pioneering industry, the games industry therefore has long experience in recognising toxic behaviour in chats or forums and taking immediate measures such as temporarily blocking users.

21 See, for example, PEGI, the Pan European Game Information System, which has defined a cross-border standard for the protection of minors.

22 For example, in the first-person shooter Battlefield 5, available at: https://www.ign.com/articles/2018/09/07/battlefield-5s-profanity-filter-is-a-work-in-progress-ea-says.

In contrast to the above aspects, the comprehensive documentation and reporting of complaint procedures and remedial measures within the meaning of the DSA is likely to represent a new task. Although some companies, such as Microsoft[23] , have been publishing transparency reports on their activities for several years, this cannot yet be considered standard practice.

According to Article 42 DSA, all moderation decisions must be documented in a comprehensible manner so that they can be reviewed if necessary. This applies in particular to the reasons for removing content, blocking user accounts and using automated moderation tools. In the games industry, this means that every decision to block an account due to cheating or toxic behaviour must be recorded in detail in a system that can be accessed by both internal teams and external auditors upon request. Some providers have already implemented technical solutions that meet the requirements of the DSA. In many cases, information and documentation about the user account is displayed. In this respect, too, the games industry already has a good foundation for complying with the DSA requirements due to its customer-centric business model in the online sector.

V. Sanctions

The DSA not only provides for new regulations, but also for sanctions. The national coordination bodies or the EU Commission are responsible for imposing these sanctions[24] .

Article 52 DSA transfers responsibility for sanctions for infringements of the DSA to the Member States and thus to the national coordination bodies, based on the powers conferred by Article 51 DSA. Member States shall adopt their own rules for this purpose, whereby the penalties shall be effective, proportionate and dissuasive and shall be determined according to the nature, gravity and duration of the infringement and the economic capacity of the provider of the digital service. The German Digital Services Act (DDG) summarises a total of 54 offences subject to fines in Section 33 DDG[25] . Most of these administrative offences can already be punished in cases of negligent behaviour – only infringements under Section 33(4) DDG require intent (Section 10 OWiG). The amount of the fines varies depending on the severity of the violation, ranging from EUR 300,000 to 6% of the global annual turnover in the last financial year, in particular for DSA violations by legal entities with a turnover of at least EUR 5 million or EUR 10 million.

In addition to the national authorities, the EU Commission is also authorised to impose fines and periodic penalty payments on VLOPs and VLSOEs (Articles 74 and 76 DSA). In the case of serious infringements, fines of up to 6% of global annual turnover will be imposed, while fines of up to 1% of global annual turnover may be imposed for less serious infringements. Intentional or negligent infringements of the DSA, interim measures or binding commitments will be sanctioned. Pursuant to Art. 74(3) DSA, a preliminary assessment by the Commission is required before sanctions are imposed. When determining the measure, particular account shall be taken of the nature, gravity, duration and repetition of the infringements. The measure must be proportionate and the prohibition of double punishment must be observed. Pursuant to Art. 77 DSA, periodic penalty payments may amount to up to 5% of the average daily worldwide turnover and serve to enforce certain measures pursuant to Art. 74(1) DSA. Fines and periodic penalty payments are subject to a five-year limitation period pursuant to Art. 77(1) and 78(1) DSA.

VI. Summary and outlook

The digitisation of public life and communication is advancing inexorably – especially in the games industry, where digital platforms create not only gaming spaces but also spaces for social interaction. With the entry into force of the DSA in 2024, European legislators are responding to this structural change and establishing a uniform set of rules for platform responsibility, user rights and digital security. The requirements apply not only to traditional social networks, but increasingly also to gaming platforms and development studios that provide hosting or intermediary services.

Platforms with high user numbers in particular – such as multiplayer hubs, games with extensive community functions or live streaming services – must prepare for complex audit requirements and possible controls by national supervisory authorities or even the EU Commission.

Companies in the gaming industry that have not yet implemented compliance mechanisms should act now and set up a robust, scalable CMS or adapt existing structures to the DSA requirements. This includes in particular:

- the systematic identification of risks, e.g. through toxic user behaviour, hate speech or the use of anti-constitutional symbols,
- clear moderation guidelines and processes for content control,
- effective internal complaint mechanisms and transparent decision documentation,
- and technical and organisational measures to make algorithmic systems transparent and trustworthy.

Regulatory developments are ongoing. It can be assumed that EU digital law will continue to evolve and expand to include new technologies such as AI-supported moderation, virtual realities and platform economies. Creating safe, fair and responsibly moderated spaces will not only be a legal imperative in the future, but also a decisive competitive factor for successful gaming platforms.

Quick read ...

- **DSA scope:** The DSA regulates online services according to size and function, including gaming platforms and communication services such as Discord.
- **Compliance management system (CMS):** Game providers must implement a CMS that includes internal processes, guidelines, training and ongoing monitoring.
- **Reporting and complaint procedures:** User-friendly systems for reporting illegal content (Art. 16 DSA) and for challenging moderation decisions (Art. 20 DSA) are important.
- **Transparency and organisation:** Regular transparency reports (Art. 15, 42 DSA) and an adapted compliance organisation are required.
- **VLOPs and sanctions:** Very large platforms have stricter obligations. Violations can result in heavy fines (up to 6% of annual turnover).

Olaf Wolters
is a lawyer at Nordemann in Berlin.

23 See Transparency Report 2024.
24 See Taeger/Pohle, Computerrechts-HdB/Paschke/Wernicke, 39. EL April 2024, Part 12, 120.4 Rn. 88.
25 See Kraul GRUR-Prax 2024, 529.

MMR

Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT

ISSN 2698-7988

Redaktion: Anke Zimmer-Helfrich, Chefredakteurin (V.i.S.d.P); Nina Himmelstoß, Redakteurin; Ruth Schrödl, Redakteurin; Christine Völker-Albert, Redakteurin; Eva Wanderer, Redaktionsassistentin; Wilhelmstr. 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: 089/381 89-427, Telefax: 089/38189-197, E-Mail: mmr@beck.de.

de.linkedin.com/showcase/zeitschriftmmr

Manuskripte und andere Einsendungen:
Alle Einsendungen sind an die o. g. Adresse zu richten. Es besteht keine Haftung für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigefügt ist. Die Annahme zur Veröffentlichung muss in Textform erfolgen. Mit der Annahme zur Veröffentlichung überträgt die Autorin/der Autor dem Verlag C.H.Beck an ihrem/seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht der Autorin/des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Peer-Review-Verfahren: Jeder Beitrag wird vor Abdruck von der Schriftleitung und ferner von zwei Gutachtern in anonymisierter Form gelesen und bewertet

Redaktionsrichtlinie C.H.Beck:
Redaktionsrichtlinien und Werkabkürzungen sind im Zitierportal des Verlags C.H.Beck abrufbar: www.zitierportal.de

Media Sales:
Verlag C.H.Beck GmbH & Co. KG, Media Sales, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München.
Media Consultants: Telefon (0 89) 3 81 89-687, Telefax (0 89) 3 81 89-589, E-Mail: mediasales@beck.de.
Auftragsmanagement: Telefon (089) 381 89-609, Telefax (089) 38189-589, E-Mail: anzeigen@beck.de
Verantwortlich für den Anzeigenteil: Dr. Jiri Pavelka.

Verlag: Verlag C.H.Beck GmbH & Co. KG, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 40 03 40, 80703 München, Telefon: (0 89) 3 81 89-0, Telefax: (089) 38189-398, info@beck.de, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX. Amtsgericht München, HRA 48 045. Persönlich haftende Gesellschafter: Dr. h. c. Wolfgang Beck (Verleger in München) und C.H.Beck Verwaltungs GmbH, Amtsgericht München, HRB 254521.

Erscheinungsweise: Monatlich.

Bezugspreise 2025: Jahresabo € 569,– (inkl. MwSt.). Vorzugspreis für Mitglieder der davit und Kooperationspartner jährlich € 435,– (inkl. MwSt.). Einzelheft € 59,– (inkl. MwSt.). Versandkosten jeweils zuzüglich. Das Abonnement beinhaltet den Zugang zum Online-Modul MMRDirekt, den Newsletter MMR-Aktuell und die MMR App. Die Rechnungsstellung erfolgt zu Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden. Jahrestitelei und -register sind nur mit dem jeweiligen Heft lieferbar.
Hinweise zu Preiserhöhungen finden Sie in den beck-shop AGB unter Ziff. 10.4.

Bestellungen über jede Buchhandlung und beim Verlag.

KundenServiceCenter:
Telefon: (0 89) 3 81 89-750,
Telefax: (0 89) 3 81 89-358.
E-Mail: kundenservice@beck.de

myclimate shape our future
chbeck.de/nachhaltig
produktsicherheit.beck.de

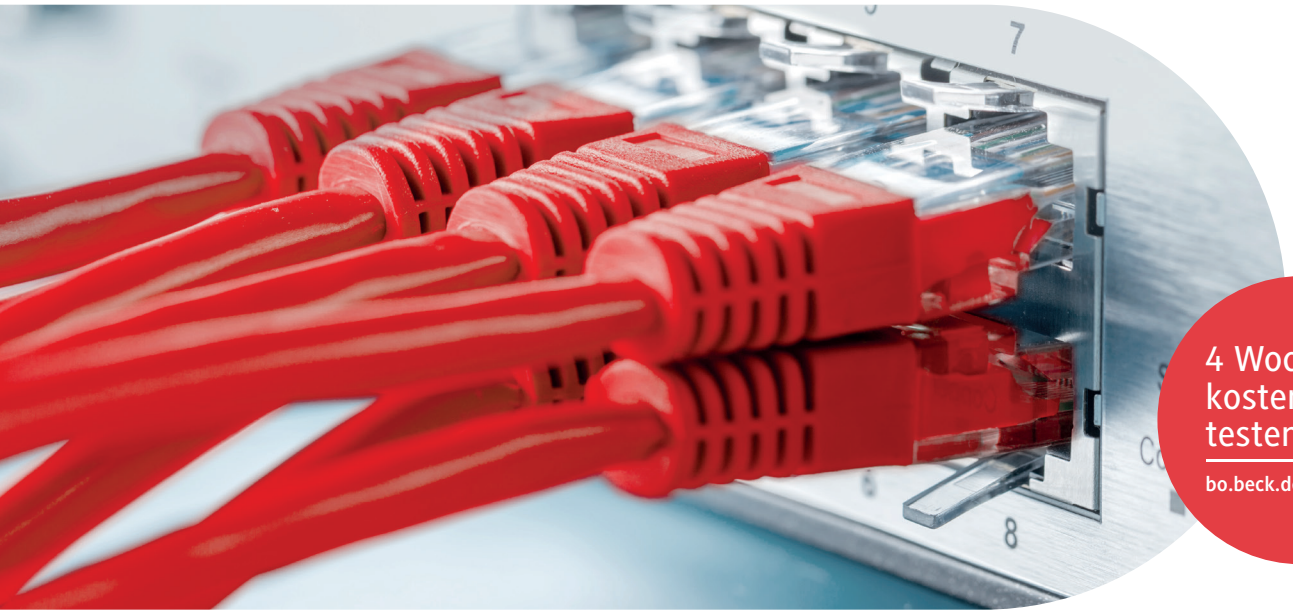
Abbestellung:
Abbestellfristen finden Sie unter: www.beck-shop.de/mmr-zeitschrift-it-recht-digitalisierung/product/1584

Hinweis gemäß Art. 21 Abs. 1 DS-GVO: Bei Anschriftenänderung kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeauftrag gestellt ist. Hiergegen kann jederzeit mit Wirkung für die Zukunft Widerspruch bei der Post AG eingelegt werden.

Satz: FotoSatz Pfeifer GmbH, 82110 Germering.

Druck: Druckerei C.H.Beck, Bergerstraße 3–5, 86720 Nördlingen.

beck-online
DIE DATENBANK



4 Wochen kostenlos testen!
bo.beck.de/0376310

Datenwirtschaftsrecht und IT-Recht

Effizient arbeiten – wann und wo Sie wollen

Schnell, sicher & smart – mit den Fachmodulen von beck-online gestalten Sie Ihre Fallbearbeitung noch rascher, effektiver und zuverlässiger.

Datenwirtschaftsrecht PLUS

Den Überblick über das immer wichtiger werdende Datenwirtschaftsrecht behalten Sie mit den zahlreichen Kommentaren und Handbüchern dieses neuen Moduls, darunter **Borges/Keil (Hrsg.), Big Data, Handbuch (Nomos), Podszun, Digital Markets Act: DMA, Paschke/Rücker, Data Governance Act sowie dem BeckOK Datenschutzrecht, Hrsg. Wolff/Brink/v. Ungern-Sternberg.**

€ 69,–/Monat* | Modulinfo & Preise online: bo.beck.de/135431

PLUS

IT-Recht PLUS

Die ideale Grundausstattung für Ihre tägliche Arbeit: Mit Highlights wie der Zeitschrift **MMR, Spindler/Schuster, Recht der Elektronischen Medien** und **BeckOK Informations- und Medienrecht, Hrsg. Gersdorf/Paal.**

€ 120,–/Monat* | Modulvergleich & Preise online: bo.beck.de/037631

PREMIUM

IT-Recht PREMIUM

Mit zusätzlichen renommierten Werken wie: **Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, Paschke/Berlit/Meyer/Kröner, Hamburger Kommentar Gesamtes Medienrecht** und **Bräutigam/Rücker, E-Commerce.**

€ 187,–/Monat* | Modulvergleich & Preise online: bo.beck.de/094931

PLUS

*Normalpreis für bis zu 3 Nutzer, Vorzugspreis teilweise verfügbar, zzgl. MwSt., 6-Monats-Abo

Verlag C.H.Beck GmbH & Co. KG, Wilhelmstraße 9, 80801 München | 174722 | Folgen Sie uns auf Mehr Infos: ch.beck.de/socialmedia
Irrtümer, Preisänderungen und Druckfehler vorbehalten.

beck-online.DIE DATENBANK genügt.

C.H.BECK