PANORAMIC

ONLINE SAFETY REGULATION

Germany

LEXOLOGY

Online Safety Regulation

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

Generated on: March 27, 2026

Contents

Online Safety Regulation

Contributors

Germany

White & Case LLP

WHITE & CASE

Markus Langen	mlangen@whitecase.com
Constantin Teetzmann	constantin.teetzmann@whitecase.com
Nicolas Bechtold	nicolas.bechtold@whitecase.com
Julius Schrader	julius.schrader@whitecase.com
Torben Harbeck	torben.harbeck@whitecase.com

LEGAL FRAMEWORK

Legal regime

Does your jurisdiction have a legal regime governing or addressing online safety? If so, how does it operate?

Apart from the EU Digital Services Act, Regulation (EU) 2022/2065 (DSA), Germany has no single piece of legislation dedicated solely to online safety, but rather a network of sectoral laws addressing different aspects of digital protection. In light of the broad scope of application of the DSA, the applicability of multiple obligations described below in parallel to the DSA still needs to be clarified.

The Interstate Media Treaty (MStV) and the Interstate Treaty on the Protection of Minors in the Media (JMStV) regulate online content, youth protection, and the prevention of harmful or illegal material, supervised mainly by State Media Agencies and the Commission for the Protection of Minors in the Media (KJM). The Telecommunications Digital Services Data Protection Act (TDDDG) governs data protection, privacy, and confidentiality in online communications in addition to the EU General Data Protection Regulation, Regulation (EU) 2016/679 (GDPR).

Beyond these, general criminal and civil law provisions – such as those on insult and defamation, incitement to hatred or personal rights – apply equally online and are enforced by ordinary courts. In cases involving criminal offences, the public prosecutor's offices are responsible for investigation and prosecution.

The German Digital Services Act (DDG) implements and supplements the DSA, for example, by designating the Federal Network Agency (BNetzA) as the national Digital Services Coordinator and establishing enforcement procedures and sanctioning powers.

Law stated - 14 November 2025

Online harms covered

Which online harms are covered under the relevant legislation and how are these harms defined?

German law addresses a broad range of online harms through specific statutes.

Under the Interstate Treaty on the Protection of Minors in the Media (JMStV), harmful online content includes content that endangers the development of minors – such as pornography, excessive violence, or content promoting discrimination or self-harm. The Interstate Media Treaty (MStV) imposes obligations on media intermediaries such as social media platforms not to discriminate against journalistic-editorial content and to maintain transparency.

In combination with the EU General Data Protection Regulation, Regulation (EU) 2016/679 (GDPR), the German Telecommunications Digital Services Data Protection Act (TDDDG) protects users from harms related to privacy breaches, unsolicited communication, and data misuse by telecommunications and digital service providers. It also provides for an information claim (sections 22-24 TDDDG) pursuant to which victims may request disclosure of user information from service providers, subject to judicial authorisation, if a criminal

offence (for example, insults or defamation or threats) has been committed via a digital service.

The German Criminal Code (StGB) covers offences such as insult and defamation (sections 185 – 187 StGB), incitement to hatred (section 130 StGB), dissemination of propaganda material of unconstitutional organisations and use of symbols of such organisations (sections 86, 86a StGB) and child sexual abuse material (section 184b StGB).

Law stated - 14 November 2025

Online services covered

Which online services are covered under the law and how are these services defined?

Beyond the DSA, the German legal framework for online safety applies to a wide range of digital and media services, in most cases depending on the relevant statute.

Under the MStV and the JMStV, the rules cover media intermediaries, video-sharing platforms, telemedia services, and broadcasters that disseminate content online. Media intermediaries are defined broadly to include services such as search engines, social networks or other platforms hosting user generated content that can influence public opinion.

The Telecommunications Digital Services Data Protection Act (TDDDG) applies to telecommunications services and digital services, including search engines or social media or other online platforms.

In addition, general criminal and civil provisions apply to any online service or platform used to publish unlawful content.

Law stated - 14 November 2025

Territorial scope

What is the territorial scope of the relevant law?

While the DSA is applicable in the entire EU, the specific German online safety framework primarily applies to services directed at users in Germany, regardless of where the provider is established.

Under the MStV and the JMStV, jurisdiction extends to foreign media and platform operators and their services insofar as they are intended for use in Germany – for example, through German-language content or marketing aimed at German users.

The TDDDG has a similar marketplace principle and applies to providers of telecommunications and digital services offered to users in Germany, even if the provider is located abroad.

Criminal law provisions, including offences under the StGB, may also have extraterritorial reach; for example, the German Criminal Code applies to crimes committed abroad by or against German citizens and if the harmful online act has effects in Germany.

Law stated - 14 November 2025

Codes of practice

Are there any codes of practice or other non-binding guidelines or recommendations relating to online safety in your jurisdiction?

In Germany, several non-binding codes of practice and soft-law instruments from regulators and industry bodies complement statutory online safety obligations.

Industry associations such as ***Bitkom*** and ***eco*** issue best-practice recommendations on online safety, including content moderation, data protection, and AI transparency.

In the area of youth protection, the Commission for the Protection of Minors in the Media (KJM) issues interpretative guidelines and decisions on content classification and the use of age verification systems. It also approves self-regulation codes developed by recognised self-regulatory organisations such as the Voluntary Self-Regulation Multimedia Services Providers Association (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V., (FSM)), which set practical standards for age-appropriate content and complaint procedures.

Law stated - 14 November 2025

Harmful versus illegal content

How does the law in your jurisdiction distinguish between harmful and illegal content?

Under German law, a distinction can be drawn between illegal and harmful online content, though in practice, there can be overlap.

Illegal content violates statutory provisions, such as criminal law or civil rights. Disseminating such content is prohibited, and online platforms are obliged to remove or disable access to it upon obtaining knowledge under the DSA.

Harmful content, by contrast, may not be unlawful but is considered inappropriate or developmentally harmful, especially for minors. It is regulated under the JMStV and covers content such as pornography, violence, discrimination, self-harm, or substance abuse. Harmful content may require age-verification or technical protection measures rather than being banned outright. Notably, the applicability of the JMStV in parallel to the DSA is disputed.

Importantly, some content can be both harmful and illegal. However, German law treats these categories separately to balance freedom of expression with youth and user protection.

Law stated - 14 November 2025

Extremist and terrorism-related content

How does your jurisdiction regulate the dissemination of extremist and terrorism-related content online?

In Germany, the dissemination of extremist and terrorism-related content online is primarily regulated under the StGB and related administrative frameworks. These national rules operate in addition to EU-level obligations, such as those under the Regulation (EU) 2021/784 on preventing the dissemination of terrorist content online. Also, Germany integrated the Directive (EU) 2017/541 on combating terrorism into its domestic law by strengthening criminal provisions on terrorism-related acts, including online dissemination and recruitment.

Extremist content includes material that incites hatred, violence, or discrimination against segments of the population, promotes unconstitutional organisations, or glorifies terrorism. Relevant provisions under the German Criminal Code include incitement to hatred (section 130 StGB), dissemination of propaganda of unconstitutional organisations and use of symbols of unconstitutional organisations (sections 86, 86a StGB) and participation in or support of terrorist organisations, including online recruitment or propaganda (section 129a StGB).

Content that falls under these categories is illegal and triggers obligations for platforms to remove it upon obtaining knowledge under the DSA.

Administrative enforcement may involve the Federal Criminal Police Office (BKA), which works with providers to identify, block, or remove terrorist or extremist content. Providers may also be subject to orders from law enforcement agencies to provide access to user information or to injunctions from courts to prevent access to such material.

Law stated - 14 November 2025

Disinformation versus misinformation

How, if at all, does the law in your jurisdiction distinguish between misinformation and disinformation online? Does it include malinformation?

In Germany, the law does not categorise online content using these terms but distinguishes content through specific legal elements in criminal and civil law.

False statements without intent (ie, misinformation) are primarily addressed by civil law statutes governing personality rights, which require negligence but no intent.

False statements with intent to harm (ie, disinformation) also trigger liability under criminal laws such as insult and defamation or incitement to hatred. These laws require intent, for example, intent to defame or to disturb public peace.

The malicious use of true facts to harm (ie, malinformation) can violate civil or criminal law, for example, laws concerning the protection of general personality rights, data protection laws or competition laws.

While the DSA addresses systemic disinformation risks, content removal depends on national law, with platforms liable only upon notice and failure to act.

Law stated - 14 November 2025

OBLIGATIONS FOR ONLINE SERVICE PROVIDERS

General obligations

What general legal obligations relating to safety are imposed on providers of online services, including providers of online intermediary services?

In Germany, providers of online services, including intermediary services, are subject to a range of general obligations relating to safety, depending on the type of service.

Civil and criminal law and other laws, such as data protection law, indirectly impose safety obligations on providers of online services in general since providers may be liable or subject to injunctions if they fail to remove or block illegal content upon notification under the EU Digital Services Act (DSA).

Under the Interstate Treaty on the Protection of Minors in the Media (JMStV), media intermediaries (eg, social networks, video-sharing platforms and search engines) must implement age verification, access restrictions, and content moderation to protect minors from harmful material such as pornography, excessive violence, or content promoting self-harm or discrimination. Notably, the applicability of the JMStV in parallel to the DSA is disputed.

The Telecommunications Digital Services Data Protection Act (TDDDG) imposes obligations on telecommunications and digital service providers to safeguard user privacy, ensure data security, and, where criminal offences are suspected, provide user information on request, subject to judicial authorisation.

Law stated - 14 November 2025

Risk assessments and mitigation

Are there any specific legal obligations for online service providers to conduct risk assessments and mitigate risks to safety?

In Germany, apart from the DSA, there are sector-specific obligations requiring online service providers to assess and mitigate risks, such as:

Under the JMStV, providers of media intermediary services (eg, social networks, video-sharing platforms) must implement protective measures, such as age verification, content filters, and access restrictions, if there is a risk of minors being exposed to harmful content. Although the JMStV does not contain any formal obligation to assess risks in this sense, such an assessment nevertheless represents a necessary preliminary step in order to be able to respond appropriately to content that is detrimental to the development of minors. Notably, the applicability of the JMStV in parallel to the DSA is disputed.

Pursuant to the Telecommunications Digital Services Data Protection Act (TDDDG), providers must implement technical and organisational measures to protect the confidentiality, integrity, and availability of data. While this is not governed as a risk assessment, compliance with these obligations requires identifying potential vulnerabilities and mitigating risks, particularly for personal data and communications.

Law stated - 14 November 2025

Protection of minors and age verification

Are there any specific legal obligations to protect minors online? If so, what measures are required or advised, such as age verification?

Germany has specific legal obligations to protect minors online beyond the requirements under the DSA, primarily set out in the JMStV, the applicability of which in parallel to the DSA is disputed. These obligations are complemented by general consumer and privacy laws and apply to media intermediaries and providers of online content that may be accessible to minors, including social networks, video-sharing platforms, and telemedia services. Key obligations and measures include the following.

- Age verification and access restrictions: providers must implement technical means to prevent minors from accessing content that is harmful to their development, such as pornography, violence, self-harm, or substance abuse. Recommended mechanisms include age verification mechanisms, verified user accounts and filtering technologies.
- Content labelling and categorisation: harmful content must be classified according to age-appropriateness to enable effective filtering and parental control.
- Risk assessment and mitigation: providers are expected to assess the potential risks to minors posed by their services and implement appropriate protective measures, proportionate to the identified risk.
- Self-regulatory guidance: organisations like the Voluntary Self-Regulation Multimedia Services Providers Association (FSM) provide codes of conduct, practical recommendations and certification schemes to help providers implement age verification and other protective measures effectively.
- Youth protection officers: commercial providers of publicly available telemedia where the services contain content which is harmful to development or harmful to minors, and providers of search engines must appoint a youth protection officer who shall serve as a contact person for users and advise the provider on matters concerning the protection of minors.

Law stated - 14 November 2025

Civil and human rights

Are there any obligations for online service providers to balance civil and human rights, such as privacy rights and freedom of expression, with safety regulations? If so, what measures are required or advised?

Under German and EU law, online service providers are required to balance civil and human rights, in particular privacy rights and freedom of expression, when applying safety and content moderation measures. These obligations include the requirements to maintain a proportionate balance between user safety, privacy, and free expression, ensuring that any restriction of rights is necessary, justified, and transparent and arises from both constitutional and statutory sources.

At the constitutional level, the Charter of Fundamental Rights of the EU and the Basic Law guarantee freedom of expression and privacy/data protection rights and the right to informational self-determination. Service providers must therefore ensure that measures to remove or restrict content are proportionate and do not unduly interfere with lawful expression.

These constitutionally protected rights are reflected in EU legislation such as the DSA and the General Data Protection Regulation (GDPR) as well as in national laws such as German civil and criminal law.

Law stated - 14 November 2025

Disinformation and misinformation

Are there any specific legal obligations to combat disinformation and misinformation online? If so, what measures are required or advised?

While the DSA requires specific online platforms to conduct systemic risk assessments and implement risk mitigation measures regarding misleading information, there are no specific German national statutory obligations that directly require online service providers to combat disinformation or misinformation as distinct legal categories. Instead, such content is addressed indirectly through general legal frameworks and obligations under national law.

Criminal and civil law may apply where false statements violate individual rights or constitute criminal offences.

Under the JMStV, the applicability of which in parallel to the DSA is disputed, content that is harmful to minors, even if not strictly illegal, must be restricted or age-gated. Risk assessments and moderation measures are advised.

In addition, public authorities and self-regulatory bodies (such as media regulators and fact-checking initiatives) promote voluntary best practices to counter false information, particularly during elections or public health crises.

Law stated - 14 November 2025

Notice and takedown

Is there a legislative 'notice and takedown' mechanism or similar in your jurisdiction? If so, how does it operate?

German law provides for a notice and takedown mechanism primarily through the DSA.

Additionally, German case law from the Federal Court of Justice (FCJ) requires hosting providers to remove unlawful content once they have obtained knowledge of the respective illegal content. Failure to act can give rise to injunctive relief or claims for damages.

Law stated - 14 November 2025

ENFORCEMENT AND PENALTIES

Enforcement

How is the online safety regime enforced in your jurisdiction?

In Germany, the online safety regime is enforced through a combination of regulatory supervision and judicial remedies.

Primary enforcement of the EU Digital Services Act (DSA) and its national framework, the German Digital Services Act (DDG), lies with the Federal Network Agency (BNetzA), which acts as the Digital Services Coordinator. The BNetzA monitors compliance with DSA obligations (except those applying to very large online platforms and search engines, which are enforced by the European Commission) and may issue orders or impose administrative fines for violations by providers established in Germany.

Regulators like the German State Media Agencies usually act through orders enforcing specific safety standards. In parallel, many media providers are Members of the Voluntary Self-Regulation Multimedia Services Providers Association (FSM), who can issue binding decisions against its members.

Users and affected parties can bring civil claims for injunctions or damages to civil courts, while criminal courts handle offences such as insult and defamation or incitement to hatred.

Law stated - 14 November 2025

Authorities

Which authorities are responsible for enforcement? What is the basis, nature and extent of their enforcement powers?

In Germany, several authorities are responsible for enforcing online safety laws, depending on the legal framework and the type of content involved. Their powers derive from both EU law (particularly the DSA and the General Data Protection Regulation (GDPR) and national legislation such as the JMStV. Notably, the applicability of the JMStV in parallel to the DSA is disputed.

The Federal Network Agency (BNetzA) acts as Germany's Digital Services Coordinator under the DSA and the German Digital Services Act (DDG). The BNetzA oversees compliance with DSA obligations (except those applying to very large online platforms and search engines, which are enforced by the European Commission), holding enforcement powers, including the ability to issue remedial orders or impose administrative fines on providers established in Germany. Also, the BNetzA acts as a central complaints office for online users, coordinates cooperation between the relevant national and European authorities, supports the EU Commission in proceedings against very large online platforms and search engines and certifies out-of-court dispute resolution bodies and trusted flaggers.

The State Media Agencies supervise together in the Commission for the Protection of Minors in the Media (KJM) online content in relation to youth protection under the JMStV. The KJM can initiate proceedings, issue administrative orders, and approve or revoke self-regulatory frameworks, for example, from the FSM.

The Federal Commissioner for Data Protection and Freedom of Information (BfDI) enforces data protection and privacy obligations under the GDPR and the Telecommunications Digital

Services Data Protection Act (TDDDG), particularly where online safety measures affect personal data.

Public Prosecutors are responsible for enforcing criminal provisions, including those relevant to online safety.

Finally, there is a plenitude of specialised agencies capable of imposing enforcement measures, such as gambling authorities for instance in cases of unlicensed online betting or market surveillance authorities, for example, with respect to toys.

Law stated - 14 November 2025

Penalties and liability

What are the potential fines or penalties for non-compliance? Are there risks of liability for employees or directors of online service providers?

In Germany, non-compliance with online safety obligations can result in administrative, civil, and, in certain cases, criminal liability.

Under the DSA and the DDG, BNetzA and the State Media Agencies may impose significant administrative fines for violations by providers established in Germany. Also, the BNetzA supports the EU Commission in proceedings against very large online platforms and very large online search engines.

Under national law, providers may face civil liability under the German Civil Code (BGB), if unlawful content hosted on their platforms infringes third-party rights and they fail to act upon notice. Plaintiffs can seek injunctive relief and damages. Also, not complying with court decisions can usually lead to fines of up to EUR 250,000.00 or imprisonment of the legal representative, if the respective fine cannot be collected.

While this is disputed, it cannot be excluded that online service providers' employees/representatives can face personal liability under German law, especially in cases of intent. For example, under the German Criminal Code (StGB), employees/representatives could be liable for aiding and abetting the respective criminal offences by not removing illegal content despite knowledge of its illegality.

Law stated - 14 November 2025

DISPUTES

Claims

What claims relating to online safety are available and most common in your jurisdiction?

In Germany, claims relating to online safety primarily arise under civil, administrative, and criminal law, depending on the nature of the alleged violation. In practice, the most common claims concern injunctive relief for general personality rights violations, data protection breaches, and insult or defamation online. The EU Digital Services Act (DSA) has introduced new administrative complaint mechanisms, which stand alongside civil and criminal remedies.

The most common civil law actions are injunctive relief and removal claims regarding illegal content, particularly under Art. 17 of the EU General Data Protection Regulation (GDPR) for data protection violations or Sections 823, 1004 of the German Civil Code (BGB) for violations of criminal law, personality rights, or intellectual property rights. In some cases, plaintiffs claim compensation for personal harm caused by personal affectedness by inadequate moderation, exposure to illegal content, or privacy violations, which is subject to strict requirements.

Under the DSA and the German Digital Services Act (DDG), users can file complaints with providers or with the Federal Network Agency (BNetzA), which can issue orders or administrative fines for violations of online safety obligations by providers established in Germany.

Users and third parties may also file criminal complaints for offences disseminated in online content such as insult and defamation (sections 185–187 StGB), incitement to hatred (section 130 StGB) or dissemination of propaganda material of unconstitutional organisations and use of symbols of such organisations (sections 86, 86a StGB). Prosecutors may investigate and pursue offenders directly.

Orders by regulatory authorities can be enforced with repeated penalties of up to €50,000 in case of non-compliance. To avoid this, the addressed providers must appeal the orders to the administrative courts.

Law stated - 14 November 2025

Procedure

What is the procedure for claimants to bring actions relating to online safety in your jurisdiction?

In Germany, the procedure for bringing actions relating to online safety depends on the type of claim (civil, administrative, or criminal) following established procedural frameworks.

Individuals may bring civil actions before the ordinary courts under the German Code of Civil Procedure (ZPO). Such actions typically seek injunctions, removal of content, or damages, and may also involve requests for preliminary injunctions to obtain swift relief. Most proceedings are preceded by out-of-court letters from claimants. Proceedings are initiated by filing a civil claim with the competent local court or regional court, depending on the value and nature of the dispute, with media and personality rights matters generally falling within the jurisdiction of the regional courts. If the parties do not mutually agree to waive it, an oral hearing is held before a judgement is issued. If the claim is successful, the judgement (such as an order to remove content, restrict access or pay damages) is enforceable under the standard rules of civil enforcement.

Complaints regarding non-compliance with the DSA or the German Digital Services Act (DDG) may be filed with BNetzA, which investigates and may issue orders or administrative fines against providers established in Germany. Users can also file complaints with the Commission for the Protection of Minors in the Media (KJM) or State Media Agencies under the Interstate Treaty on the Protection of Minors in the Media (JMStV).

Orders by public authorities often require an administrative appeal prior to the case being brought to the courts.

Where conduct amounts to a criminal offence, victims or affected parties may file a criminal complaint with the police or the public prosecutor's office, initiating a formal investigation and prosecution.

Law stated - 14 November 2025

Remedies

What interim and substantive remedies may be imposed in relation to online safety claims?

In Germany, both interim (preliminary) and substantive remedies are available to address online safety concerns.

Interim remedies (preliminary measures)

Courts may grant preliminary injunctions ordering platforms to promptly remove, block, or restrict access to illegal content. In matters involving violations of personality rights, German courts usually presume the urgency necessary for such injunctions. Although it is not mandatory to initiate substantive proceedings concurrently, a preliminary injunction may be revoked, for example, after the lapse of a certain period or if the applicant fails to commence main proceedings despite a court order. Alternatively, the parties may agree to treat the injunction as final and binding.

Providers addressed by orders from public authorities need to appeal these orders in the form of requests for preliminary injunctions to reduce enforcement risks as administrative orders are often immediately enforceable.

Substantive remedies

Courts can issue orders requiring providers to remove, block or restrict access to unlawful or harmful content. Additionally, while such claims are subject to strict requirements (including a serious violation of personality rights and a demonstrated necessity for monetary compensation), courts can award damages to victims as financial redress for harm suffered as a result of unlawful content or insufficient content moderation by online service providers.

Law stated - 14 November 2025

Defences and exemptions

Does your jurisdiction provide any defences or exemptions from liability for online safety claims? If so, how do they operate and which online services providers may avail of them?

Most importantly, German law provides one defence and exemption from liability for online service providers, particularly in the context of content hosted by third parties. Under the

DSA, providers are generally not liable for content they do not create or control, provided they act promptly to remove or block access once they obtain actual knowledge of illegal content. This is commonly referred to as the hosting provider privilege.

This hosting provider privilege applies in cases in which the providers do not have actual knowledge of the illegal content. In most cases, this knowledge is established through a notification sent to the provider. However, German courts have repeatedly held that a notice of illegal content must meet specific requirements, providing the online service provider with knowledge of facts that make the illegality of the content apparent without the need for a detailed legal or factual assessment. The notice must contain a sufficiently specific reference to enable the provider to readily identify and affirm the violation.

This defence generally applies to hosting providers, social media platforms and other intermediaries, but does not extend to providers which generate illegal content.

Law stated - 14 November 2025

UPDATE AND TRENDS

Key trends and future developments

What are the most noteworthy recent trends and developments in online safety regulation in your jurisdiction? What developments are expected in the coming year?

Germany's regulatory landscape for online safety has evolved significantly in recent years, with notable recent trends and anticipated developments shaping the future of digital content moderation and user protection. Two specific trends are the intermediary services' obligation to remove identical and core-similar content upon notice and the regulation of AI-generated content.

A significant recent development in Germany's content moderation framework concerns the scope of the obligation to remove illegal content after obtaining knowledge of its illegality. Some German courts recently confirmed intermediary services' obligation to not only remove certain illegal posts accessible via a specific URL subject to a notification but also to remove identical and core-similar content from their platform and to prevent the re-uploading of such content. This approach aims to address the recurrence of illegal material by leveraging technical measures to detect and remove identical and core-similar content proactively. While this obligation enhances user protection, it also raises concerns about the hosting provider's privilege, the potential over-removal of content and the challenges of balancing safety with freedom of expression.

The rise of AI has introduced new challenges in online safety, particularly concerning AI-generated content. Risks arising from generative AI are now at the forefront of regulatory attention. For example, the European Commission has requested information from major platforms under the EU Digital Services Act (DSA) about how they mitigate generative-AI harms (deepfakes, automated summarisation and election risks). In addition, ongoing litigation is already testing the limits of liability for AI-generated content and fundamental-rights proportionality.

On the national legislative side, Germany is preparing market-surveillance measures to implement the EU AI framework with the German AI Market Surveillance and Innovation

Promotion Act and to align DSA enforcement with the forthcoming AI Act regime, creating overlapping supervisory responsibilities.

Any views expressed in this publication are strictly those of the authors and should not be attributed in any way to White & Case LLP.

Law stated - 14 November 2025