Baker McKenzie.

Client Alert

May 2026

Germany: Draft Act to Combat Digital Violence

In brief

This article is of practical relevance for technology companies operating in Germany - providers of online platforms (social networks, video-sharing platforms, marketplaces), web-hosting and cloud-hosting services, and internet access providers (IAPs). On 16 April 2026, the German Federal Ministry of Justice ("**BMJ**") published the ministerial draft of an Act to Strengthen Civil and Criminal Protection against Digital Violence ("**GgdG-E**"). Industry submissions are due by 22 May 2026.

The draft proposes three new criminal offenses targeting deepfakes, image-based sexual abuse and digital surveillance, and — more importantly for the day-to-day operations of intermediaries — a stand-alone civil-law regime allowing affected individuals to obtain disclosure of user identity, evidence-preservation orders, and judicial account suspensions. Non-EU social networks must continue to appoint a domestic service agent on pain of fines of up to EUR 500,000 (EUR 5 million for legal entities). The civil-law regime will contain specific deletion duties and procedural requirements that materially change how intermediaries must handle user data in this context.

Contents

Background

The GgdG-E intends to implement an undertaking from the current coalition agreement and is, in part, the German vehicle for transposing Articles 5 and 6 of Directive (EU) 2024/1385 on combating violence against women and domestic violence (image-based sexual abuse and stalking enabled through information and communication technology – ICT). The draft pursues two parallel pillars: a **criminal-law pillar**, which will add three new offenses to the German Criminal Code ("**StGB**"); and a **civil-law pillar** in the form of a stand-alone act — the GgdG — which will create rights for affected persons against intermediaries and IAPs.

The criminal-law pillar — three new offenses

The planned criminal-law amendments are most directly addressed to individual perpetrators, but technology companies whose products may be used to commit these offenses should evaluate product design and content-moderation measures accordingly.

§ 184k StGB (revised) — Violation of intimate privacy through image recordings. The provision is recast as the central StGB rule on image-based sexual abuse. It criminalizes (up to two years' imprisonment or a fine) the unauthorized creation or third-party disclosure of images depicting sexual acts, uncovered intimate body parts, sexually-determined images of clothed intimate body parts, and — critically — images modified or combined with other content via a computer program so as to create the impression of

any of the above (i.e., sexualized “deepfakes”). The existing requirement that the recording take place in a space protected against view is dropped; after this amendment, recordings made in publicly accessible areas such as saunas, beaches and changing rooms will be in scope.

§ 201b StGB (new) — Violation of personality rights through deceptive content. The provision will criminalize the unauthorized making available to third parties of computer-generated or computer-altered content that creates the impression of depicting an actual event involving another person and is suitable to cause significant damage to that person's reputation. It is the legislator's response to the limits of existing law (notably § 33 of the Art Copyright Act, “KUG”) when applied to convincing AI-generated content. The provision is technology-neutral, will capture non-sexualized deepfakes, will apply to depictions of deceased persons, and is subsidiary to other provisions carrying a heavier penalty.

§ 202e StGB (new) — Unauthorized surveillance via ICT. The provision will criminalize the repeated or continuous unauthorized monitoring of another person's location or activities via ICT, where the conduct is likely to cause serious harm. The rule targets in particular GPS trackers, stalkerware, and analogous tools. Vendors of legitimate tracking, fleet-management, parental-control or anti-theft technologies should review whether default settings, consent flows and technical safeguards reliably keep their products outside the offense's reach.

The civil-law pillar — the GgdG

The civil-law pillar is the most operationally significant part of the draft for technology companies. The GgdG creates a self-contained set of claims that affected individuals can pursue in the German Regional Courts (Landgerichte) against intermediaries and IAPs, regardless of whether the intermediary is itself liable for the underlying content. If implemented, the GgdG will have the following key features:

1. Personal scope

The GgdG will apply to “service providers” and IAPs (§ 1(2) and (3) GgdG-E). The category of service provider includes (i) online platforms within the meaning of Art. 3(i) DSA (i.e., social networks, video-sharing platforms, marketplaces), (ii) web-hosting services that allow users to publish websites, and (iii) cloud-hosting (file-hosting) services. The account-suspension claim under § 4 and the domestic-service-agent obligation under § 9, by contrast, are confined to “social networks”, a narrower subset of online platforms (§ 1(4)). Mere conduit and caching services, search engines, and purely interpersonal communication services such as messengers and email are not in scope.

2. The “infringement” gateway (§ 1(1))

An infringement within the meaning of § 1(1) GgdG-E will exist where (i) a service of a covered provider has been used to commit (ii) an act fulfilling one of an enumerated list of offenses, and (iii) the act is not justified. The catalog covers the principal “digital violence” phenomena — hate speech, doxing, cyber-stalking, image-based abuse, defamation, threats and identity misuse — and **is somewhat broader than the catalog under the former NetzDG.**

3. Disclosure of user data (§ 2)

Upon prior judicial order from the competent Regional Courts, intermediaries and IAPs will be obliged to disclose to the affected person the data necessary to enforce civil claims against the user. The disclosure set is meaningfully broader than under existing procedures: in addition to subscriber-level personal details (name, date of birth, address, e-mail, telephone), it includes the IP address (with port number) used at the time of the infringement and the IP address used at the time of the last login before the order was served, in each case with timestamp. Where the IP address obtained from the platform is dynamic, the IAP will then be ordered to allocate it to a subscriber and disclose the subscriber data. The applicant will be required to credibly show the underlying facts and state an intention to bring a civil claim.

4. Evidence-preservation orders and the new deletion regime (§ 3)

Once a § 2 procedure is pending and there are sufficient factual indications of an infringement, the competent court must, ex officio and without delay, issue an order to the intermediary (i) not to delete the data falling within the disclosure set, and (ii) to make a copy of the challenged content. The provider will be required to transmit the preserved data and content copy directly to the court in text form. The court will then be required to issue a parallel order to the IAP, requiring it to allocate the IP/port to a subscriber and to store the resulting subscriber data pending completion of the procedure.

The deletion regime that follows is one of the most operationally consequential provisions of the draft. Under § 3(5) GgdG-E, once the disclosure procedure has been finally decided, the court must notify the provider and the IAP. If the provider/IAP is ordered to disclose, it must irreversibly delete (or ensure the irreversible deletion of) the preserved data and content copy after providing disclosure. If the provider/IAP is not ordered to disclose, it must irreversibly delete those items already upon receiving the court's notification. The explanatory memorandum makes clear that “irreversible” deletion must be guaranteed in line with the state of the art — fragments capable of reconstruction are not sufficient. Other statutory storage powers and obligations are expressly preserved.

In practice, intermediaries will need to design preservation workflows that segregate GgdG-related data from other data sets, and to maintain audited deletion procedures that can demonstrate compliance with the post-procedure deletion duty without prejudicing other retention obligations. The data preserved under § 3 may not be disclosed to the applicant unless the procedure is finally resolved in the applicant's favor; it may, however, be transmitted to criminal-prosecution authorities. Outside these uses, the data may not be processed for any other purpose.

5. Account suspension (§ 4)

The most novel — and most controversial — element of the GgdG is the new claim for judicial suspension of user accounts in social networks. Where a user commits an infringement that severely impairs the affected person's personality rights, the affected person will be able — subject to a court order — to require the social network to suspend all known accounts of the user, for a reasonable period, where this is necessary to prevent further infringements. “Suspension” means that the user can no longer post, comment or share content; passive read-mode use must remain available. The provider will also be required to prevent — to the extent technically and economically reasonable — the user from opening and operating new accounts during the suspension period.

Suspension will be “regularly necessary” (§ 4(3)) where the user fails to provide or breaches a cease-and-desist undertaking, or where other indicators give rise to a fear of further infringement. The court must consider whether milder content-moderation measures (e.g., demotion, demonetization, partial restrictions) would suffice. § 4(4) clarifies that the GgdG-E claim does not preclude the provider from suspending accounts on a contractual basis or under Art. 23(1) DSA without a judicial order.

6. Domestic service agent (§ 9)

The draft retains and recalibrates the obligation, originally found in § 5 NetzDG, for non-EU social networks to designate a domestic service agent. Under § 9(1), social networks not established in an EU Member State must designate a domestic service agent and prominently identify the agent in their offering, at the latest when the service is offered in Germany. Non-compliance will be an administrative offense punishable by up to EUR 500,000; for legal persons, the cap rises to EUR 5 million. For EU-established social networks, by contrast, the GgdG-E (consistent with C-376/22) will only allow a court to require designation of a domestic service agent on a case-by-case basis for a specific pending proceeding.

Tension with the Digital Services Act

The BMJ devotes a substantial portion of the explanatory memorandum to arguing that the entire scheme is compatible with the DSA. The argument rests primarily on Art. 6(4) DSA (preservation of national authority orders against illegal content), recital 25 (DSA liability exemptions leave injunctive remedies untouched), and recital 34 (national courts may issue disclosure and content orders on a national-law basis). On this view, both the disclosure procedure and the account-suspension claim are “orders to act against illegal content” rather than horizontal regulatory obligations.

Art. 23(1) DSA addresses provider-side regulatory obligations to suspend services to users that “frequently” provide manifestly illegal content. However, the GgdG-E claim, by contrast, could arise on a single severe infringement where there is a risk of repetition. The BMJ takes the position that Art. 23 does not exclude civil-law claims between private parties; whether that view holds — particularly in light of the DSA's full-harmonization objective — is likely to be tested in the Technical Regulations Information System (TRIS) notification procedure and may ultimately reach the CJEU. Service providers in scope should anticipate a period of legal uncertainty rather than a settled regime.

Practical takeaways for technology companies

Intake and triage. Disclosure and preservation orders under §§ 2 and 3 will be issued by Regional Courts. Trust-and-safety, legal and engineering teams will need defined workflows to receive, validate and act on these orders within the short response windows the draft contemplates.

Data retention. The disclosure set under § 2(2) will require providers to surface IP addresses (with port number) at both the time of the infringement and the time of the last login before service of the order. Providers should map current retention practices against this set, taking into account the parallel proposed reform of § 174 of the Telecommunications Act ("**TKG**") and the contemplated quick-freeze IP-retention regime.

Post-procedure deletion. The § 3(5) GgdG-E deletion duty will require irreversible deletion of preserved data and content copies in defined scenarios. Data segregation, audit logging and verifiable deletion processes will be necessary to demonstrate compliance — especially where the same data is also subject to other retention obligations. It is highly questionable whether a mere geo-block will meet the obligation.

Account-suspension processes. Social networks should ensure their existing trust-and-safety processes can accommodate court-ordered suspensions covering all known accounts of a user, including effective measures to prevent new-account creation during the suspension period (within the "technically and economically reasonable" limit).

Domestic service agent. Non-EU social networks should confirm that their existing service-agent appointments under the legacy § 5 NetzDG will satisfy the new § 9 GgdG requirements, and ensure visibility of the agent designation in the German offering. EU-established social networks should be prepared to designate a domestic service agent on judicial order on a case-by-case basis.

Product design. Vendors of generative-AI image tools, location-tracking products, parental-control software and similar offerings should review consent flows, default settings and abuse-mitigation features in light of the new criminal law provisions (see above).

Outlook

Industry submissions are due by 22 May 2026, after which the draft must clear cabinet, the parliamentary procedure and the TRIS notification procedure with the European Commission. The notification procedure is likely to expose the draft's most ambitious provisions — in particular § 4 GgdG-E — to closer scrutiny on full-harmonization grounds. The civil-law pillar is to be evaluated five years after entry into force; adoption is targeted for 2026.

Your Contact

Sebastian Schwiddessen LL.M.
Counsel
sebastian.schwiddessen@bakermckenzie.com