

RULING

ECJ Russmedia ruling: The end of liability privilege for hosting providers?

Blog article



December 2025

Author: Dr. iur. Sarah Bischof,
Attorney at law, VISCHER AG

ECJ RUSSMEDIA RULING: THE END OF LIABILITY PRIVILEGE FOR HOSTING PROVIDERS?

In its judgment C-492/23 of 2 December 2025 (Russmedia), the European Court of Justice examined whether a hosting provider, namely Russmedia, must proactively take action against content that violates personality rights if it qualifies as a controller under data protection law. Some interpret this ruling as the end of the liability privilege, which requires such service providers to take action against illegal content that is unknown to them only after receiving a notification (notice-and-take-down). However, this appears to be based on a misunderstanding of the ECJ's reasoning.

In this article, we will assess this reasoning and also explain the corresponding legal situation in Switzerland.

THE LIABILITY PRIVILEGE IN THE EU

The eCommerce Directive, in force since 2000, already introduced the principle of "no liability without knowledge" in the EU. In short, this principle means that a service provider is not liable for user-published content if:

- the service in question consists merely of storing that very content on behalf of the user (**hosting**);
- it has **no actual knowledge** of illegal content; and
- it **swiftly removes or blocks** illegal content upon becoming aware of it.

This privilege is justified by the fact that the hosting provider plays a purely passive, technical, and neutral role.

The Digital Services Act (**DSA**) has since incorporated this liability rule, which continues to apply there in the same form.

WHAT HAPPENED IN THE RUSSMEDIA CASE?

The case originated from an advertisement on an online portal operated by Russmedia. An anonymous user posted an ad (falsely) offering sexual services, using the data subject's real and her private mobile phone. Although Russmedia promptly removed the advertisement upon the data subject's request, she subsequently sued Russmedia for non-material damages. After proceedings through several national courts the case reached the ECJ.

The ECJ was asked to clarify the following problem: Can a hosting provider that also commercially uses content published by its users still benefit from the liability privilege, or must it ensure compliance with data protection law (namely the General Data Protection Regulation, GDPR) in connection with the personal data published on its platform?

WHAT DOES THE ECJ SAY?

First of all, the ECJ concluded that Russmedia is considered a (joint) controller under data protection law for the content published on its online portal. Specifically, Russ media's terms of use reserved the right to "use, distribute, transmit, reproduce, modify, translate, pass on to

partners and remove at any time" published content. The Court found this reservation alone provided decisive "*indications*" that Russmedia processes the data not only for the advertising user, but also for of its own commercial interest. Thus, participating in determining the purposes and means of the original publication. In addition, the ECJ's noted that Russmedia has a significant influence on the worldwide dissemination of the personal data contained in the advertisements by determining the parameters for their distribution on its platform according to the target audience and determining, among other things, the presentation and duration of the publication.

The supposed "bombshell" of the judgment, however, is the ECJ's subsequent conclusion that a hosting provider that is a controller for the published content under data protection law cannot invoke the liability privilege of the eCommerce Directive (now the DSA). In the ECJ's opinion, Russmedia should have proactively identified special categories of personal data (such as information about sexual life in this case) and ensured that only the data subject themselves or someone with their consent published it. Additionally, Russmedia should have used appropriate technical measures to prevent the copying and dissemination of this data.

The ECJ did not address whether Russmedia actually knew of the personal data in question, i.e., whether it actually used the disputed advertisement for its own commercial purposes. Rather, the ECJ based its view on the fact that Directive 95/46/EC (the GDPR's predecessor expressly excluded questions it covered from the scope of the eCommerce Directive (which was applicable at the time the disputed advertisement was published) (Art. 1(5)(b) and recital 14 of the eCommerce Directive).

The current DSA also expressly leaves the provisions of the GDPR unaffected (Art. 2(4)(g) DSA); it can therefore be assumed that the ECJ would have reached the same decision under the new DSA regime.

HOW SHOULD THE ECJ'S REASONING BE ASSESSED?

The judgment and its reasoning are comprehensible and ALIGN with the intentions of the European legislator.

However, the ECJ's reasoning omits an important point: A service provider can only benefit from the liability privilege under the eCommerce Directive/DSA if its service consists of "*storing information provided by a user on their behalf*" (cf. Art. 14(1) eCommerce Directive and Art. 3(g)(iii) DSA). The privilege therefore clearly relates only to the hosting itself.

This means the following:

- If the hosting provider uses the published content for its own commercial purposes, then at least this subsequent own use can no longer be considered a "hosting" service. The liability privilege clearly cannot apply to such downstream processing.
- However, a service provider also leaves its passive intermediary role, and must consequently lose the liability privilege, if it co-determines significant decisions about the "why" and "how" of the publication of the data on its platform and thus becomes at least jointly responsible for this process under data protection law. This view corresponds with the established ECJ case law, which regularly qualifies platform operators as joint controllers with their users for the publication or collection of data,

provided they have a significant influence on the data collection and processing via the platform's function and parameterisation (see [Facebook-Fanpage-Judgment](#) (C-210/16) and [Fashion ID-Judgment](#) (C-40/17)).

It is important to note that the ECJ did not affirm Russmedia's role as a joint controller solely because the company reserved the right in its terms of use to use the third-party content for its own purposes; rather, it considers this as an indication. The decisive criterion for assuming joint responsibility was instead, in this case too, the active and determining participation in the publication of the user content, which resulted from the specific design and parameterisation of the platform. By creating the technical and organisational framework for the data publication and thus pursuing its own economic interests, Russmedia significantly influenced the purposes and means of the processing. Therefore, even applying the ECJ's case law in the Russmedia judgment, a service provider does not become a (joint) controller merely by contractually reserving the right to use published content for its own purposes; further co-determination is required.

The provision in the eCommerce Directive/DSA that the applicable data protection law remains unaffected, on which the ECJ relies in the Russmedia judgment, must also be understood against this background: Anyone who is obliged under the GDPR to ensure lawful data processing should not be able to evade this responsibility by invoking the liability privilege.

The above is likely to be primarily relevant for online marketplaces, social networks and similar services, as on the one hand these service providers have an inherent interest in organising and preparing user-published content, for example to increase the attractiveness of its own platform. On the other hand, the service provider on such platforms often has more influence over the design of data collection and processing than, for example, with a pure web-hosting provider, whose service is primarily limited to the provision of storage space.

The question therefore arises as to whether a service provider must confine itself to the purely passive, technical and automatic storage of information if it does not want to avoid liability for its users' illegal content. Recital 22 of the DSA offers at least some guidance in this regard, stating that a hosting service provider may index and catalogue the information provided by users and stored at their instigation in order to make it findable via a search function integrated on its platform, without this alone imputing actual knowledge of the content. This clarification is crucial as it acknowledges that certain activities that go beyond pure storage are essential for the provision of a functional and user-friendly service. It can therefore be assumed that an additional function or service that goes beyond pure storage but still serves the user's purpose – namely the effective accessibility of their content to third parties – does not automatically disqualify the service provider from invoking the liability privilege. The decisive criterion is whether the service provider maintains a neutral, technical, and passive role or whether it assumes an active one that gives it knowledge of or control over the specific content. As long as an additional function (such as indexing) is automated and occurs without editorial or curatorial intervention that would suggest a substantive engagement with the content, the passive character of the service is maintained.

The parallel to data protection law, in particular the distinction between controller and processor, underpins this conclusion. If a hosting provider designs such an additional function or service in such a way that the associated processing of personal data is carried out

exclusively for the purposes and on the instructions of the user, the hosting provider is not considered a controller from a data protection perspective, but a processor (see Art. 4 No. 8 GDPR). Classifying the hosting provider as a processor strongly indicates that it also assumes a passive role under today's DSA and can therefore invoke the liability privilege. The ECJ's reasoning in the *Russmedia* judgment reinforces this view.

In summary, it can be said that the "explosive force" of the *Russmedia* judgment lies not in the undermining the liability privilege, but rather in the fact that it takes up an aspect of provider liability that may have been overlooked in practice until now. In our opinion, it must continue to be possible for hosting providers to reserve the right to use the published user content themselves. However, in light of the ECJ's reasoning in the *Russmedia* ruling, it is advisable for hosting providers to clearly identify and delimit such uses as their own processing operations in order to reduce as far as possible the appearance of involvement in the publication of content by users.

HOW WOULD THE FACTS BE ASSESSED IN SWITZERLAND?

In contrast to the EU, Switzerland has no specific liability regulation for hosting providers or similar service providers, such as is now enshrined in the DSA. The draft of the new [Federal Act on Communication Platforms and Search Engines](#) (CommPA; currently not available in English), which the Federal Council put out for consultation at the end of October 2025, only provides for an obligation on communication platforms to set up a reporting procedure, but no associated relief from liability.

Consequently, the civil liability of hosting providers for user content that violates personality rights is governed by the general provisions of tort law in Art. 41 et seq. of the Code of Obligations (CO), the protection of personality rights in Art. 28 et seq. of the Civil Code (CC) and the Data Protection Act (DPA). For claims by data subjects in the event of data protection violations that also constitute a violation of personality rights, the DPA refers back to the provisions of Art. 28 et seq. CC.

The interplay of these norms results in the following, differentiated regime of responsibility and liability:

- A person whose personality rights have been violated may, in accordance with Art. 28 and 28a CC, demand the removal of the unlawful situation from anyone contributing to the violation. Federal Supreme Court has established that mere participation objectively constitutes a violation, even if the person acting is not or cannot be aware of it ([BGE 141 III 513, E. 5.3.1. with references](#), only available in German). In a more recent decision, the Commercial Court of Zurich concluded that the operator of a search engine could facilitate the finding of content that violates personality rights, but that this was not sufficiently closely related to the act itself; "influencing" was not sufficient, actual "participation" was required ([Decision of the Commercial Court of Zürich HG220030-O of 21 August 2024, E. 3.2.4.2.6](#), only available in German).
- When content that violates personality rights is published on a hosting provider's platform, the provider supplies the technical infrastructure for the violation. In contrast to the operator of a search engine, a hosting provider's service is much more

closely related to the infringing content and thus has a causal effect on its dissemination and maintenance, even without specific knowledge of the published content. This form of participation is regularly sufficient to justify a claim for removal directly against the hosting provider. The data subject can therefore demand the deletion or removal of the infringing content from the service provider. This claim exists irrespective of fault and also applies if the hosting provider acts merely as a data processor for the user from a data protection perspective.

- However, in order for the data subject to also be able to assert a claim for damages or satisfaction against a hosting service provider under Art. 41 et seq. CO in conjunction with Art. 28a para. 3 CC, fault on the part of the provider must be proven in addition to the damage, unlawfulness and a causal link. According to prevailing doctrine and in line with legal developments abroad, such fault (usually negligence) is only assumed if the hosting provider remains inactive despite a sufficiently concrete and substantiated notification of the obviously illegal content and does not immediately remove or block it. Thus, a *notice-and-take-down obligation* de facto also applies in Switzerland, which is also anchored in relevant industry standards (see for example the [Code of Conduct Hosting \(CCH\)](#), which was developed by Swiss hosting companies under the leadership of Swico). As long as the hosting provider has no knowledge of an infringement and acts promptly upon notification, this liability privilege protects it from claims for damages. This view has however not yet been confirmed by the courts.
- The aforementioned liability privilege is also subject to the condition in Switzerland that the provider assumes a passive role as a mere technical intermediary. If the hosting provider also uses the content published by its users – in particular personal data – for its own purposes (e.g. for personalised advertising, creating user profiles, its own analyses or passing on to third parties), it abandons this passive role. It appropriates the content and, just as in the EU, becomes the controller for the downstream processing in the sense of the DPA and is also fully liable for any violations of personality rights.
- We are currently not aware of any Swiss court judgments that have addressed the question of the degree of "co-determination" from which a hosting provider also becomes (jointly) responsible for the publication of user content on its platform. Experience shows, however, that Swiss courts are guided by the case law of the EU, which is why it is highly probable that Swiss courts would also classify a provider like Russmedia as a joint controller for the publication of user content. Nevertheless, it is also likely to be the case in Switzerland that a provider does not become a joint controller for the publication solely by the fact that it contractually reserves the right to use user content for its own purposes, but that further concrete acts of participation would be required.
- As a (joint) controller for the publication of user content, the provider must proactively ensure compliance with data protection principles from the outset. This includes in particular the obligation to ensure the lawfulness of data processing (Art. 6 paras. 1 and 2 DPA) and the accuracy of the personal data processed (Art. 6 para. 5 DPA). The provider must therefore ensure on its own initiative that the data it uses for its own

purposes was collected lawfully and is factually correct. These proactive, statutory obligations of a controller conflict with the reactive nature of the *notice-and-take-down principle*. A controller cannot claim ignorance of a violation of personality rights, as its role requires it to check the lawfulness of the data processing for which it is responsible. Failure to conduct such a check already justifies the accusation of negligence if the provider reserves an active role for itself through the design of its services and terms of use. Consequently, the liability privilege, which was created for the passive intermediary, can therefore not apply to the provider who appropriates the data through co-designing of the data processing and also (but not solely) reserving rights of use, even according to the principles prevailing in Switzerland.

Based on the points set out above, it is therefore probable that a Swiss court would reach a similar conclusion to the ECJ in the Russmedia case, provided that the hosting provider can be proven to be jointly responsible for the publication of user content. We therefore advise Swiss hosting service providers to take steps to avoid, as far as possible, such (joint) responsibility for user content. This includes, among other things, clearly distinguishing between any use for the hosting provider's own purposes and the publication by the user, so as not to give the impression of participation. If a participation and, therefore, joint responsibility is unavoidable (for example, because it is inherent in the business model), robust compliance processes should be implemented to meet the hosting provider's data protection obligations as a controller and thus minimise liability risks.

Dr. iur. Sarah Bischof, Attorney at law, VISCHER AG

Zurich, December 2025



The IAB (Interactive Advertising Bureau) Switzerland Association represents the digital marketing and advertising industry in Switzerland and supports the industry in achieving success in the world of digital advertising.

The association is objectively and actively committed to knowledge transfer, standards, transparency and quality in digital advertising, and informs its stakeholders and, where necessary, the general public about developments and issues relating to the digital marketing and advertising industry. Its members include agencies, media companies, advertisers and technology companies.

Through cooperation with other Swiss communications associations, the IAB advocates for its members and promotes the interests of the digital advertising industry to legislators and political decision-makers. In particular, the IAB advocates for framework conditions that support the financing of journalistic content through advertising and aims to address the use of data and AI in the advertising industry from an economic and social perspective.

In this role, the IAB acts as the primary point of contact for information relating to the digital marketing and advertising industry and ensures an optimal exchange of ideas and knowledge through its training and further education courses, conferences and specialist events. In cooperation with its global sister associations and the IAB Tech Lab, the IAB develops and disseminates technical standards and solutions.



VISCHER is a law firm offering a wide range of services, including in the field of digital marketing. VISCHER partner Rolf Auf der Maur is a member of the IAB Advisory Circle and practices as a lawyer in the areas of online law, media, and technology. Sarah Bischof is an attorney at law at VISCHER. She practices primarily in data law, particularly with regard to issues in the field of online marketing.