

# ECJ Strengthened Data Protection on Online Marketplaces

Thomas Wahl

News

On 2 December 2025, the Grand Chamber of the European Court of Justice (ECJ) ruled in *Case C-492/23 (Russmedia Digital and Inform Media Press)* that the operator of an online marketplace is responsible for processing the personal data contained in advertisements published on its platform.

## Background of the case

The victim of an advertisement with defamatory and offensive content, which had been published by an unknown person on the online marketplace "www.publi24.ro", is demanding non-material damages from the operator, Russmedia Digital (a Romania-based company). According to the advertisement, the person concerned was offering sexual services. The advertisement contained photos and the telephone number of the person concerned. Russmedia Digital removed the material within an hour after the victim's request, as the advertisement was untrue and harmful to her. However, the advertisement was quickly picked up by other websites, where it remained accessible. Russmedia argued that its role is purely technical, merely providing a hosting service. However, it reserves the right to use the content.

The referring Court of Appeal of Cluj, Romania, sought guidance from the ECJ as regards the obligations on the operator of an online market place under the [General Data Protection Regulation \(GDPR\)](#) and as regards the question of whether such an operator may be relieved of those obligations on the basis of the exemption from liability provided for by Art. 14(1) of [Directive 2000/31](#) for intermediary service providers.

## The ECJ's reasoning

The ECJ justifies its [ruling](#) as follows: Although the advertisement is placed by a user, it is only published via the online marketplace on the internet and thus made accessible to internet users. Therefore, before publishing these advertisements, the operator of an online marketplace must take appropriate technical and organisational measures to identify those advertisements that contain sensitive data and verify that the user who is about to place such an advertisement is the person whose sensitive data is contained therein.

If this is not the case, they must verify whether the person whose data is being published has expressly consented to the publication. Without this consent, the operator of an online marketplace must refuse to publish the advertisement in question, unless it falls under one of the other exceptions provided for in the GDPR.

## AUTHOR

Thomas Wahl

Senior Researcher  
Max Planck Institute for the  
Study of Crime, Security and  
Law

---

Preprint eucriM 2025, Vol. 20(4)  
ISSN: 1862-6947  
<https://eucriM.eu>

---



In addition, the operator of an online marketplace must endeavour to prevent advertisements containing sensitive data published on its website from being copied and unlawfully published on other websites. To this end, it must take appropriate technical and organisational security measures.

Lastly, the ECJ clarified that the operator of an online marketplace cannot avoid its obligations under the GDPR by relying on the exemption from liability under the regime of Directive 2000/31. It follows from a combined reading of Art. 1(5)(b) of Directive 2000/31 and Art. 2(4) of the GDPR that the provisions of the Directive, in particular Arts. 12 to 15 thereof, cannot interfere with the regime under the GDPR.

#### Put in focus

Art. 6 of the [Digital Services Act \(DSA\)](#) and Art. 14(1) of Directive 2000/31 (the "e-commerce Directive") include the so-called "provider privilege". Accordingly, where an information society service is provided that consists of the storage of information provided by a recipient of the service, that service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information. The GDPR does not contain such a clause. As a result, it has been under dispute whether the provider privilege also covered the processing of personal data.

The ECJ has now resolved this conundrum unilaterally in favour of the GDPR. The ruling could have far-reaching consequences for the internet. In any case, it increases the pressure on service providers to carry out preventive checks.

---

## About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.

All news items are freely accessible at: <https://eucrim.eu/news/>

Stay informed by emailing to [eucrim-subscribe@csl.mpg.de](mailto:eucrim-subscribe@csl.mpg.de) to receive alerts for new releases of issues.

The project is co-financed by the [Union Anti-Fraud Programme \(UAFP\)](#), managed by the [European Anti-Fraud Office \(OLAF\)](#).



**Co-funded by  
the European Union**