



Nestor Nestor Diculescu Kingston Petersen  
ATTORNEYS & COUNSELORS

Legal & Tax



# GDPR | A year under review

Our top picks of past and upcoming judgements of the Court of Justice of the European Union

26 May 2025



# Our top judgements of the Court of Justice of the European Union

(26 MAY 2024 – 25 MAY 2025)

1

## Judgement in the Case C-621/22 - Koninklijke Nederlandse Lawn Tennisbond

- ➔ **What the Court mainly said:** According to the CJEU, a purely commercial interest regarding data processing can be considered as a “legitimate interest” if certain conditions are met. Thus, this legitimate interest does not have to be laid down by law, but it must be lawful, and the processing of the data concerned will be allowed when strictly necessary, without less intrusive alternatives. In addition, a balancing test between the interest of the controller and the rights of the data subjects will be required, while the data subjects must be able to reasonably foresee the use of their data.
- ➔ **What are the practical implications:** If the organizations refrained until now to rely on a legitimate interest as a legal basis in case of purely commercial interests, they can rely on it now, provided the criteria laid down in the Court judgement are met. In case organizations already rely on the legitimate interest as legal ground in case of purely commercial interests, they must assess if the requirements set forth by the Court judgement are already met and, if not, comply with them or change the legal ground.

2

## Judgement in the Case C-446/21 – Maximilian Schrems

- ➔ **What the Court mainly said:**

The CJEU held, amongst others, that a situation in which a person states his/her sexual orientation during a panel discussion open to public does not qualify as processing of personal data “manifestly made public by the data subject”, as provided under the safeguard from Art. 9 para. 2 letter (e). Therefore, in this case, a social media platform operator is not entitled to process other data related to sexual orientation obtained outside the platform (from third-party websites or apps) based on such safeguard.
- ➔ **What are the practical implications:** Organizations must be cautious when processing special categories of data. Even if a person publicly discloses any special categories of data regarding him/her in the context of a public discussion or in other similar situations, this is not sufficient to trigger the application of the safeguard indicated at Art. 9 para. 2 letter (e) (“manifestly made public by the data subject”), so

that the controller must identify another safeguard under Art.9 or refrain from processing such special categories of data.

## 3

## Judgement in the Case C-169/23 – Másdi

- **What the Court mainly said:** The Court referred to the applicability of the provision under Art. 14 para. (5) letter (c) of GDPR. This is an exemption from the obligation to inform data subjects, which is triggered where obtaining or disclosing the data is expressly provided by law (to the extent it provides appropriate measures to protect data subjects' legitimate interests). Thus, the CJEU stated in its judgement that the aforesaid GDPR exemption applies to the personal data, regardless of the way in which they were obtained. Accordingly, if the exception previously mentioned is applicable, the controller is not required to inform the data subject about the data obtained from a third party or the data generated by the controller itself in the course of its tasks.
- **What are the practical implications:** Organizations can rely on this exception to avoid the information obligation for the personal data irrespective of their source (obtained from third parties and data generated internally). However, organizations must clearly identify the specific legal provision allowing the processing and ensure that the measures necessary to protect the legitimate interests of data subjects are effectively implemented. Such assessment on the applicability of the exemption under Art. 14 para (5) letter (c) must be adequately documented, as required by the responsibility principle.

## 4

## Judgement in the Case T-354/22– Bindl v Commission

- **What the Court mainly said:** According to the Court, the data subjects may be entitled to compensation not only for material damage but also for non-material damage suffered as a result of a violation of the data protection rules. In this specific case, the Court considered that the transfer of data outside the European Economic Area (EEA) without the adequate transfer mechanisms in place created an actual and certain non-material damage for the data subject, since it put him in a position of uncertainty with regard to the processing of his personal data. Moreover, the Court deemed that there is a sufficiently direct causal link between the data protection violation and the non-material damage suffered by the data subject, assessing that such non-material damage amounts to EUR 400 to be paid by the controller who transferred his data outside EEA.
- **What are the practical implications:** Further to this Court ruling, organizations should strengthen their data protection practices, as even minor violations can lead to compensation claims. This includes, amongst others, ensuring proper security measures, clear internal procedures, periodical trainings of personnel and efficient communication with affected data subjects.

# Our top upcoming judgements of the Court of Justice of the European Union

1

## Judgement in the Case C-693/22 - I. (Vente d'une base de données)

- **What the matter mainly refers to:** The Court must consider whether, under the GDPR, a national law that permits the sale of a database containing personal data in enforcement proceedings, even when the data subject has not consented to the sale, is permissible.
- **What are the practical implications:** If the Court aligns the Advocate General's position and allows the sale of a database containing personal data without the data subjects' consent, provided such processing is deemed necessary and proportionate to enforce a civil law claim, several practical implications arise. First of all, it could reduce the level of control that data subjects have over their personal data. Moreover, determining whether such data processing meets the thresholds of necessity and proportionality may introduce legal and procedural uncertainty, particularly in the absence of clear criteria or oversight mechanisms.

2

## Judgement in the C-654/23 - Inteligo

- **What the matter mainly refers to:** The CJEU must interpret, amongst others, whether Art. 83 paragraph 2 of the GDPR means that a supervisory authority imposing an administrative fine is required to assess and explain within the sanctioning document the impact of each of the criteria provided at letters (a) to (k) of such article upon the decision to impose a fine and, respectively, upon the decision with regard to the amount of the fine applied.
- **What are the practical implications:** Depending on the answer of the Court, supervisory authorities may need to redraft their sanctioning document templates or at least to change the manner in which such documents are filled in, so as to reflect therein the criteria employed in determining both the decision to impose a fine and the specific amount of the fine. In this case, organizations may have a reason to challenge the sanctioning document if the supervisory authorities do not adequately explain such sanctioning criteria.

## Judgement in the Case C-492/23 – Russmedia

- **What the matter mainly refers to:** The CJEU has to distinguish between the qualification as processor or controller in the context of storage and hosting online information, in order to determine in the light of this clarification what their obligations are under the GDPR. Among other matters, the Court will determine to what extent the controllers are responsible for (i) verifying the identity of the person posting ads and for carrying out prior checking of the content of ads which are potentially unlawful or likely to infringe a person's private and family life, as well as for (ii) implementing technical measures to prevent unauthorized copying and redistribution of those ads.
- **What are the practical implications:** If the Court adopts the position of the Advocate General, storage and hosting providers would be considered, in the light of the GDPR, as processors regarding the ads posted by the users, and therefore would not be obliged to proactively monitor the content of the ads or implement technical measures to prevent copying or redistribution, thus limiting their responsibilities for user-generated content. However, for registered users advertisers, the platform operators would act as controllers and must verify their identity, as well as comply with the obligations laid down by the GDPR for data controllers in relation to them, such as ensuring a valid legal basis for processing, providing clear privacy notices, and applying adequate security measures.

## Judgement in the Case C-413/23 P – EDPS v SRB

- **What the matter mainly refers to:** The case covers the situation in which only the controller disclosing certain pseudonymized information is able to identify the data subjects, while this is not possible for the recipient of such information. Thus, the information pseudonymized by the disclosing controller cannot be correlated by the recipient with additional information which would identify data subjects. In this case, we expect that the Court will also clarify, among others, whether the privacy notice provided to data subjects must also cover the disclosure of such pseudonymized information to the recipient for whom such information is not personal data.
- **What are the practical implications:** If the CJEU follows the Advocate General's position that pseudonymised data represents personal data, organizations must treat such data as fully subject to data protection rules, even when shared with third parties who cannot directly re-identify data subjects. This means they must comply with transparency obligations, including informing data subjects about the disclosure of their personal data, identifying all the categories of recipients and ensuring that this information is provided clearly and in an efficient manner.

## Authors



**Iurie Cojocaru**  
**Partner**  
Head of the Data Protection practice  
E: [iurie.cojocaru@nndkp.ro](mailto:iurie.cojocaru@nndkp.ro)



**Oana Ștefan**  
**Associate**  
Data Protection practice  
E: [oana.stefan@nndkp.ro](mailto:oana.stefan@nndkp.ro)



**Diana Albu**  
**Associate**  
Data Protection practice  
E: [diana.albu@nndkp.ro](mailto:diana.albu@nndkp.ro)

## NNDKP Data Protection Practice

NNDKP's Data Protection practice stands out as a premier choice for navigating the ever-changing legal landscape in the data protection and privacy field. NNDKP was among the first Romanian law firms to recognize the significance of this field, establishing a dedicated practice in 2008. This forward-thinking approach translates into unmatched expertise for our clients.

Our team is comprised of highly skilled and experienced lawyers who are passionate about data protection. We understand the complexities of compliance and the ever-increasing demands businesses face. This allows us to provide comprehensive advice and a strategic approach that addresses our clients' unique needs.

More details about our expertise are available [here](#).

*Note: This document should not be copied, disclosed, distributed or reproduced, in whole or in part, without the prior written consent of Nestor Nestor Diclescu Kingston Petersen. The contents of this document is for information purposes only and should not be relied upon or construed as legal or other kind of advice. Professional advice should therefore be sought before any action is undertaken based on this document.*

Check out NNDKP's Data Protection blog for latest news and valuable insights into the data protection field.

[Read more](#)

