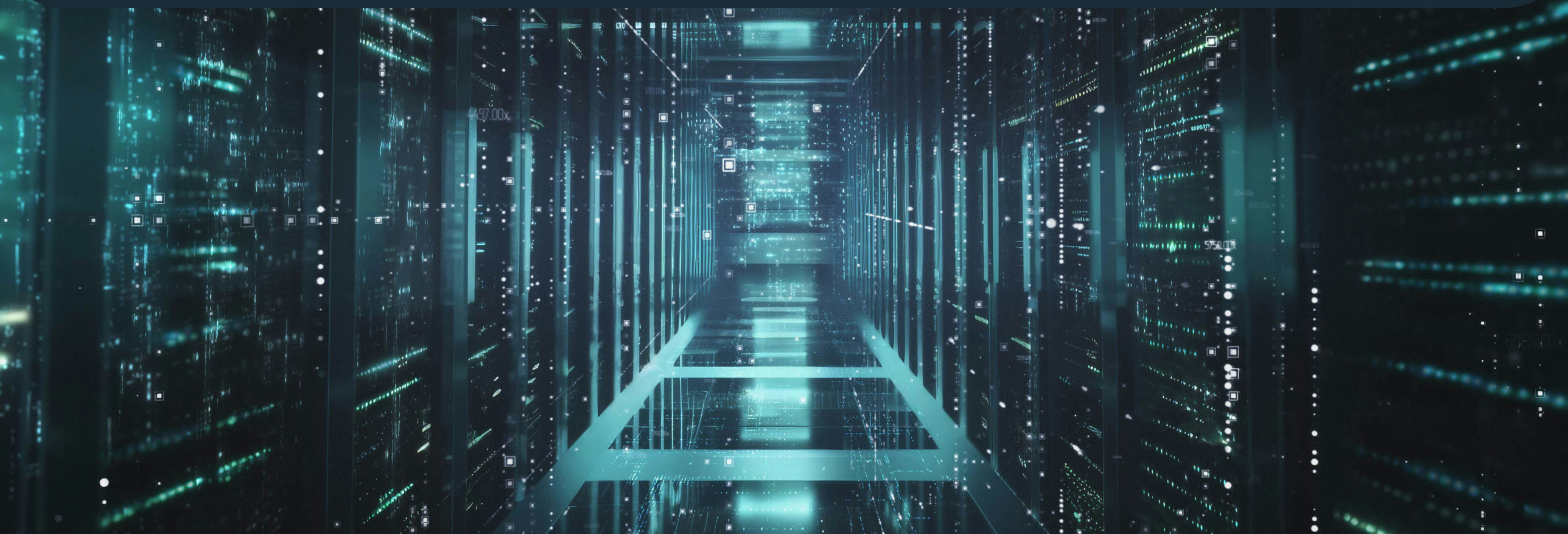
14 Issue 2026

Legance

New case law on the use of unlawfully obtained personal data in civil proceedings



In its judgment of 18 June 2026 (Case C-484/24), the Court of Justice of the European Union addressed the relationship between **data protection rules** and **the use of personal data as evidence in civil proceedings**. The case arose from a dispute between a German employer and a former employee, whom the employer accused of selling company assets through her private online marketplace account after the termination of her employment. According to the referring court, the employer allegedly discovered those sales after accessing the former employee's private account using her login credentials. The employee challenged both the employer's conduct and the use of the information obtained in this way, prompting the referring court to seek guidance on whether personal data collected through a potentially unlawful processing may subsequently be relied upon as evidence in judicial proceedings.

Against this background, the referring court asked, among other things, whether the GDPR requires national courts to exclude evidence obtained through an unlawful processing of personal data and whether Article 17(3)(e) GDPR constitutes an autonomous legal basis for the subsequent use of such data in judicial proceedings.

The CJEU answered both questions in the negative. It held that **the GDPR does not establish a general exclusionary rule preventing national courts from considering evidence solely because it was obtained through an unlawful processing of personal data**. Instead, **the admissibility of evidence remains governed by the applicable national procedural rules**, provided that the relevant national legal framework complies with EU law.

At the same time, the Court emphasized that the absence of a general rule of inadmissibility does not exempt judicial authorities from complying with the GDPR. Once personal data are introduced into judicial proceedings, the court itself carries out a separate processing operation that must independently satisfy the requirements of the Regulation. Accordingly, compliance with the GDPR must be assessed not only in relation to the original collection of the data, but also in relation to their subsequent processing by the judicial authority. In particular, courts must ensure that the processing is based on an appropriate legal basis under Article 6 GDPR, while Article 17(3)(e) GDPR merely provides an exception to the right to erasure and does not constitute an autonomous legal basis for processing.

The Court further clarified that judicial authorities must comply with the principles of necessity and data minimization throughout the proceedings. This requires **courts to assess whether all personal data contained in the evidence are genuinely necessary for deciding the dispute** and, where appropriate, **to limit the disclosure of unnecessary information** or adopt measures such as anonymization or pseudonymization, particularly where documents contain information relating to third parties or where judicial decisions are made publicly available.

The judgment provides further guidance on the interaction between data protection rules and national procedural law, confirming that the GDPR does not itself regulate the admissibility of evidence while reaffirming that the subsequent processing of personal data by judicial authorities remains subject to the safeguards and principles established by the Regulation.

Italy, for example, adopted a specific rule (art. 160-bis of the Italian Privacy Act) which sets forth that "*The validity, effectiveness and admissibility in legal proceedings of acts, documents and orders based on the processing of personal data that does not comply with*

the provisions of the law or the GDPR remain governed by the relevant procedural provisions" which, in cases similar to the one appraised by the CJEU, has often determined that, in order to admit personal data within the trials, labour courts consistently ascertain the compliance with privacy laws of the data retrieval and collection by the employers; in a slight departure from this tendency, a recent ruling by the Court of Pisa (issued on 13 June) held that any administrative unlawfulness relating to the storage of email logs and communications did not, in the circumstances of the case, prevent the employer from relying on that information in the proceedings concerning the dismissal of an employee. In doing so, the mentioned Court recalled the guidance provided by the Court of Cassation on the doctrine of the so called "defensive controls" which, under strict limits, allows targeted and ex-post investigation on employees' working devices (and related data) by the employers.

The matter, however, remain not entirely settled, with the Italian Data Protection Authority repeatedly taking stark contrasts with the employers even when they access and process employees' data on a limited basis and for defensive purposes, where such processing is not

preceded by full information notices and prior trade union agreement or administrative authorization on tools and devices – including the email's metadata – that the authority by default considers as monitoring tool. The matter is less contentious outside the labour law disputes area where the violation of privacy laws will not necessarily determine the inadmissibility in different civil or criminal proceedings.

For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it

Martina Balzani
mbalzani@legance.it