Landmark decision of the ECJ on the anonymisation of personal data

04.09.2025

Jobs

+++ Please find the German version below. +++

ECJ clarifies when anonymised data is available

In its ruling of 4 September 2025, the European Court of Justice (ECJ) clarified when anonymised data is available and thus effectively specified the applicability of the GDPR. The appropriate de-

It is true that it can be inferred at first glance from recital 26 in the preamble to the GDPR that it does not apply to anonymised data. However, long before the GDPR came into force, the dispute arose over when anonymization of data in the legal sense can exist at all. In the judgment of 19 October 2016, the Breyer case, the ECJ ruled that IP addresses can constitute personal data if controllers have ways of obtaining customer data from Internet providers. This decision has already had a fundamental impact on data protection on the global Internet. The ECJ is now continuing this case law and thus clarifying this question.

The abstract question of when anonymization exists revolves around the problem of what means are available to a responsible body to identify (or "re-identify") a person behind a data set. It is conceivable that another body has the linking element – as is the case with IP addresses, as Internet providers can assign them to their customers. This is also the question that arose in the current legal dispute between the European Data Protection Supervisor and the Single Resolution Board (SRB). The SRB had shared creditor data with a third-party company in a resolution procedure of a Spanish bank, whereby the personal reference was replaced by an alphanumeric code. The persons concerned were not informed about this transfer. The European Data Protection Supervisor argued that only pseudonymized data exists, even if the third-party company cannot identify the individuals, as the identifiers could only be assigned by the SRB. The ECJ decided, once again, in favour of the approach that takes the respective perspective of a responsible body: from the point of view of the SRB, pseudonymised (and thus personal) data is available, but from the point of view of the third-party company, anonymised data to which the GDPR does not apply.

However, information obligations remain in place

However, the ECJ further ruled that the SRB had to inform the persons concerned about the transfer, since at least from its point of view the personal connection was given. This decision is understandable and welcome, as it continues to provide clarity for data subjects as to which bodies receive their data and why, if necessary, they do not have to comply with the GDPR.

Anonymization of cross-industry interest

The problem of how to anonymize data in a legally compliant manner arises in numerous are
For example, this question comes up again and again in medical or statistical research data
can also be very relevant when training AI models or the application of AI systems, as ano
zed data sets are GDPR-compliant training and output data.
At the same time, affected persons are not left defenceless. Anonymization must mean anonymity and exclude the dangers of re-identification. Those entities that hold the necessary key for re-identification must fully apply the provisions of the GDPR. Those bodies that hold anonymised

+++

Landmark decision by the CJEU on the anonymization of personal data

In its ruling of September 4, 2025, the European Court of Justice (CJEU) clarified when data is considered anonymised, thereby effectively specifying the applicability of the GDPR. This appropriate decision is a continuation of the CJEU's line and sets another milestone in a highly controversial legal issue.

At first glance, it appears from recital 26 of the GDPR that it does not apply to anonymised data. However, long before the GDPR came into force, there was already controversy over when data can be considered anonymised in the legal sense. In its judgment of October 19, 2016, in the Breyer case, the CJEU ruled that IP addresses can constitute personal data if controllers have the means to obtain customer data from internet providers. This decision already had a fundamental impact on data protection on the global internet. The CJEU is now continuing this case law and thus clarifying this issue.

The abstract question of when anonymization exists revolves around the problem of what means are available to a controller to identify (or "re-identify") a person behind a data record. It is conceivable that another body may have the linking element – as is the case with IP addresses, since Internet service providers can assign them to their customers. This question also arose in the current legal dispute between the European Data Protection Supervisor and the Single Resolution Board (SRB). In a resolution procedure involving a Spanish bank, the SRB had shared creditor data with a third-party company, replacing the personal reference with an alphanumeric code. The individuals concerned were not informed of this transfer. The European Data Protection Supervisor argued that only pseudonymised data was available, even if the third-party company could not identify the individuals, as the codes could only be assigned by the SRB. The CJEU once again opted for the approach that takes the perspective of the respective controller: from the SRB's point of view, the data is pseudonymised (and therefore personal), but from the third company's point of view, it is anonymised data to which the GDPR does not apply.

Jobs

However, information obligations remain in place

However, the CJEU further ruled that the SRB had to inform the data subjects about the tra as it considered the data to be personal. This decision is understandable and welcome, as it continues to provide clarity to data subjects as to which entities receive their data and why, in some cases, these entities are not required to comply with the GDPR.

This question arises repeatedly in the context of medical or statistical research data, but can also be very relevant in the training of AI models or the application of AI systems, as anonymised data sets are training and output data that comply with the GDPR.

At the same time, data subjects are not left unprotected. Anonymization must mean anonymity and exclude the risks of re-identification. Those entities that hold the necessary key to re-identification must fully apply the provisions of the GDPR. Those entities that hold anonymised data must continuously monitor that the applicability of the GDPR is not revived by the fact that re-identification is suddenly possible again through new means.

More on the topic

Trade

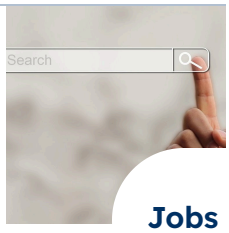
12.03.2025

Guest access in online retail – Higher Regional Court of Hamburg confirms HmbBfDI

Your right to data protection

08.11.2024

News on the right to be forgotten – current decisions of the Federal Court of Justice and the ECJ

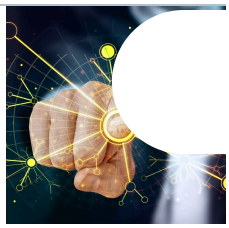


Jobs

Current court decisions

07.12.2023

Impact of the Schufa ruling on AI applications



Der Hamburgische
Beauftragte für Datenschutz
und Informationsfreiheit

ECJ strengthens right to free initial copy of patient file

all news →

Address

The Hamburg Commissioner for
Data Protection and Freedom
of Information, Ludwig-Erhard-Str. 22,
20459 Hamburg

Contact

(040) 428 54 - 4040 (Telephone HamburgService)

mailbox(at)datenschutz.hamburg.de

Service

File a complaint

Report a data breach

Data protection officer to register/deregister

Jobs

Legal

Privacy policy

Accessibility Statement

Jobs