


Dr. rer. oec. Katja Gehrke,
Institut für deskriptive Gesundheitsdatenanalyse OHG (DGDA)
ORCID 0000-0001-5516-457X
Dr. jur. Joachim Jung
Möhrle Happ Luther Rechtsanwälte

CJEU ruling: new freedoms for SHI data

>> With § 25b of Book V of the German Social Code (SGB V), the legislature has allowed health and long-term care insurance funds to analyze existing data to protect the health of their insured persons. The aim is to detect risks earlier and point insured persons to suitable preventive and treatment options. This changes the role of social data. They no longer serve only billing or documentation. They can also help identify future risks. Not the illness itself, but the risk becomes the reason for contacting insured persons.

What § 25b SGB V permits

§ 25b SGB V is not a general license for unrestricted data use, but has a clear purpose: protecting the health of insured persons. Health insurance funds may analyze data if this serves to identify risks and point insured persons to appropriate services.

The provision names specific cases: rare diseases, cancers, risks from medicinal products, comparably serious health risks, vaccination indications and the detection of a not yet established need for long-term care. The legislature thus does not want to permit just any use of data. It wants to enable earlier and better care.

At the same time, § 25b SGB V sets limits. Insured persons must be informed and must be able to object. The use must not serve to select risks or deny benefits. Notices are meant to help, not to stigmatize. A score must not become a covert instrument of steering.

This is precisely why § 25b SGB V is an important test case. The provision shows how a solidarity-based system can deal with predictions. Data should be used, but not against insured persons.

Why external service providers matter

Analysis under § 25b SGB V requires robust models. Such models do not emerge by themselves. They must be developed, tested and continuously improved. Health insurance funds have the data. External service providers often have the necessary expertise in statistics, software and model validation. It is therefore obvious for funds to commission such providers.

Under data protection law, this is usually done through commissioned data processing, which § 25b(2) sentence 5 SGB V expressly provides for. The fund remains fully legally responsible. The service provider may use the data received exclusively for developing the models and not for any other purposes.

This makes a first point important: External developers were already able to develop risk models under § 25b SGB V for health insurance funds. For this development, the service provider generally does not need the identity of the insured persons. A model learns from patterns. It analyzes, for example, diagnoses, medicines, hospital stays, indications of care needs or subsequent events. Names, addresses or insurance numbers regularly do not help here. What matters is whether a reliable pattern emerges from many cases.

This leads to the central question: Does the external developer need to receive personal data at all? Or is a dataset sufficient in which the fund removes the direct link to a person and retains the key for re-identification?

What the CJEU changes

This is where the ruling of the Court of Justice of the European Union (CJEU) of September 4, 2025, in Case C-413/23 P becomes important. The CJEU clarified that pseudonymized data need not necessarily constitute personal data subject to strict data protection requirements for every person and every recipient.

What matters is the perspective of the specific recipient: If the recipient can identify the data subject by means reasonably available to it, the data remain personal for that recipient. If, however, it has no access to the key and no other legally and practically usable means of re-identification, the data may lack a personal reference from its perspective.

This is the core of the so-called "relative" concept of personal data. It is not only the dataset that matters. It also matters who receives it and what means that body can actually and legally use.

More than commissioned processing

For § 25b SGB V, this distinction is of practical importance. Developing a model as a processor was already possible. What is new is the question of whether the external service provider can also use pseudonymized data beyond the individual assign-

References

1. Urteil des Gerichtshofs (Erste Kammer) vom 4. September 2025, Rechtssache C-413/23 P, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62023CJ0413
2. Stoklas, J. (2025) EuGH: Personenbezug – absoluter oder relativer Ansatz bei pseudonymisierten Daten? In ZD-Aktuell, Jahrgang 15, Nr. 20, 01442, 31.10.2025
3. Grosmann, P./ Luh, C. (2025) Datenschutzrecht: Regeln zur Weitergabe pseudonymisierter Daten, EuZW, S. 1103
4. Golland, A. (2025) Regeln zur Weitergabe pseudonymisierter Daten mit Personenbezug, NJW, S. 3415
5. Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG) 2024, Bundesgesetzblatt 2024 I Nr. 21 vom 25. März 2024, abrufbar unter: https://www.recht.bund.de/bgbl/1/2024/101/VO.html?utm_source=chatgpt.com
6. Kühling, J./Buchner, B. (2024) Datenschutz-Grundverordnung/BDSG. Kommentar. 4. Auflage, München: C.H. Beck
7. He, Z. (2023): From Privacy Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law. European Journal of Law and Technology, 2, Art. 17. DOI: 10.1007/s44206-023-00043-5, abrufbar unter: https://doi.org/10.1007/s44206-023-00043-5
8. Bundesministerium für Gesundheit (2026) Referentenentwurf eines Gesetzes für Daten und digitale Innovationen im Gesundheitswesen (GeDIG), abrufbar unter: https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/gedig

Citation

Gehrke, K., Jung, J.: "CJEU ruling: new freedoms for SHI data", "Monitor Versorgungsforschung" (05/26), pp. 56–57.
http://doi.org/10.24945/MVF.05.26.1866-0533.2860

ment, because the data transmitted by the fund fall outside data protection law from its perspective.

Such further uses may include improving its own models, testing new methods or developing general tools for risk detection. This goes considerably further than classic commissioned processing.

CJEU case law may open up new scope here. The prerequisite, however, is that the service provider cannot reasonably identify the insured persons. The data may then fall outside data protection law for the provider. It would then not be bound merely because the data are personal data for it.

This does not mean, however, that the data may be used at will. Contracts, social law, confidentiality protection and the trust of insured persons remain important. The fund must also be able to explain why it passes on data in this form and for what purposes. The CJEU ruling is therefore no carte blanche. But it does create new room for legally sound models of cooperation.

Why this matters for innovation

It is precisely here that CJEU case law can create new scope. Classic commissioned processing remains the safe default for the primary development of § 25b algorithms. What is new, however, is a second option: If the health insurance fund transmits datasets in a form in which the external service provider cannot reasonably restore the personal reference, the recipient may use these datasets freely for further innovation or quality assurance purposes, as it is not bound by data protection requirements. This freedom of further data use exists only if the fund has not restricted use for other purposes.

This may give rise to a new role for service providers – no longer merely the fund's extended arm, but a partner for better methods. This can improve care, because many models get better when developed and tested with larger and more diverse datasets. False alarms can decrease. Risks can be detected earlier. Biases can also be checked more effectively, for example when a model performs worse for certain age groups or groups of insured persons.

Pseudonymization must be robust

This new option stands or falls with the quality of pseudonymization. A dataset is not unproblematic simply because it is labeled pseudonymized. It must be examined whether the recipient truly cannot identify the individuals.

This requires asking simple but important questions: Does the dataset contain rare diagnoses, small groups or conspicuous courses of disease? Can age, region and treatment pathway together make a person identifiable? Does the service provider have access to other data that facilitate attribution? Are there clear prohibitions on re-identification? Are these prohibitions safeguarded technically? Is it checked whether the provider's employees could use other sources?

The more sensitive the data, the stricter this examination must be. Health data are particularly worthy of protection. Even if they no longer have a personal reference for the service provider, the trust of insured persons remains crucial. A fund must be able to show that no covert change of purpose is taking place.

Clear rules, not data release

In practice, a clear separation is therefore advisable. In a first step, the external developer can develop a model for the fund as a processor. This processing remains closely bound to § 25b SGB V. In a second step, it can be examined whether a dataset can be prepared in such a way that the service provider can no longer identify the insured persons. Only then can further uses be considered.

This separation should be safeguarded not only technically but also contractually. The key for attribution must not be held by the service provider. Access to additional data must be excluded. The permitted purposes must be clearly described. In addition, it should be documented why re-identification cannot reasonably be expected.

Other rules also remain important. Depending on purpose and application, the EU AI Act may also play a role. If a system is used for medical purposes, medical device law may also become relevant. Relief under data protection law thus does not mean that no rules apply anymore. It merely shifts the focus: away from the mere question of personal reference toward quality, control and accountability.

Outlook

§ 25b SGB V shows where the use of social data is heading. Data should not merely reflect past services. They should help detect risks earlier and plan care better.

External service providers will play an important role in this. As processors, they were already able to develop such models. Beyond that, the new CJEU case law may open up new avenues. If data are transmitted in such a way that the developer cannot reasonably identify the insured persons, the personal reference may cease to exist in the view of the Luxembourg judges. Uses that go beyond the individual assignment then also become possible.

The opportunity lies in better models and more innovation. The risk lies in unclear purposes, weak oversight and lost trust. The task in the coming years will therefore not only be to make data usable. It will also be to create clear rules for their use. Only then can § 25b SGB V become an instrument that detects risks early, improves care and protects insured persons at the same time.

Moreover, various current legislative developments show that, under certain conditions, existing data are to be and can be used more extensively, which may contribute to improved healthcare and steering in the future. <<