German Social Insurance
European Representation
50 Rue d'Arlon
1000 Brussels
Belgium

Phone: +32 2 282 05-50
info@dsv-europa.de
www.dsv-europa.de
Transparency Register ID:
917393784-81

Deutsche Sozialversicherung
Europavertretung | DSV

Opinion from German Social Insurance issued 23 February 2026

Proposals of the European Commission on omnibus legislation in the digital field

I. Preliminary remarks

The German Social Insurance (DSV) welcomes the initiative of the European Commission to simplify and harmonise the multitude of existing legal acts in the digital field through a Digital Omnibus. Social security institutions, with their own IT infrastructures, data-intensive administrative processes and the prospective use of artificial intelligence (AI) systems, are faced with the task of integrating the requirements of the relevant legislation into their governance and compliance structures at an early stage and on a sustainable basis. Clear, coherent and user-friendly regulation is therefore essential in order to deploy digital innovations in a legally secure manner while at the same time ensuring the high standards of data protection and social security in Europe.

Against this background, DSV recognises that the proposed Regulations provide for important steps towards the harmonisation of digital regulatory frameworks – such as a postponement of the timelines for high-risk AI, uniform requirements for data protection impact assessments, the modernisation of cookie rules or the envisaged streamlining of reporting structures. Such measures can simplify implementation and enhance legal certainty.

At the same time, however, DSV emphasises the special protection that must be afforded to social data. Some of the proposed amendments in data protection law concern key definitions and may also affect the protection of social data. For the social insurance, it is essential that the high standards of protection for social data are maintained and that new rules do not lead to legal uncertainty or to a lowering of the established level of protection.

II. Position

1 _ Artificial intelligence

DSV supports the objective of the European AI regulatory framework to enable innovation while at the same time protecting fundamental rights and European values. For social security institutions, legal certainty in dealing with Regulation (EU) 2024/1689 (AI Act) as well as planning certainty are of central importance, as high-risk AI systems may in particular be used in benefit decisions and rehabilitation management. In view of the delayed availability of the required standards, DSV

therefore welcomes the intention to postpone the date of application of the provisions for high-risk AI and to link it to the availability of supporting instruments, including the necessary standards. However, an extension of the implementation period must not lead to an interim shift of risks related to the use and processing of such systems. This means that any extension of transitional periods can only be justified if binding minimum requirements regarding transparency, explainability and technical and organisational measures, as well as risk-based impact assessments for the use of such systems, already apply in advance.

Furthermore, DSV welcomes the proposed amendment to Article 6(4) of the AI Act. According to this, the registration obligation pursuant to Article 49(2) does not apply to providers of AI systems listed in Annex III if, on the basis of a documented assessment, they conclude that the system is not high-risk.

DSV also positively assesses the expansion of compliance instruments through additional regulatory sandboxes, including an EU-wide sandbox from 2028. These offer opportunities for early testing of governance, risk and data protection requirements as well as for pilot projects in the field of rehabilitation and prevention. Regulatory sandboxes thus constitute a valuable instrument for the operational implementation of AI compliance, for example for testing human-in-the-loop approaches, documentation as well as the interplay between data protection and fundamental rights impact assessments. Early involvement of social security institutions is desirable.

In light of the particular need to protect social data, DSV emphasises that the proposed simplifications and graduated obligations in the AI framework for small and medium-sized enterprises (SMEs) and start-ups must not lead to a weakening of transparency, explainability and accountability requirements. This applies in particular where AI systems are used by third parties on behalf of or in the context of social security institutions. In areas with a high relevance for fundamental rights – such as the social and health sectors – it is therefore necessary, from the perspective of DSV, to limit exemptions for SMEs accordingly and to clarify that minimum data protection standards, risk assessments and adequate documentation of data processing operations must be fully ensured.

In addition, DSV considers a clear distinction between AI use in the public sector serving the public interest and commercial profiling practices to be necessary, particularly with regard to purpose limitation, transparency, relevance for decision-making and the possibility of objection or correction. Especially in exploratory machine learning processes, technically unavoidable intermediate steps – such as the generation of scores or probabilities at the level of individual entities – should not

be prematurely classified as profiling, in order to ensure legal certainty and not to hinder innovation.

2 _ Data governance, data access and data protection

Social security institutions not only provide social data for research purposes but also require reliable access to data themselves in order to ensure continuity of services. The simplification and harmonisation of rules on data governance, data access and data protection envisaged by the Digital Omnibus can, in principle, contribute to improving the responsible use of data for research, prevention and service management, and to facilitating the implementation of large-scale digital projects. From the perspective of social security institutions, there is therefore a strong interest in the creation of high-quality and secure data spaces in which, in particular, pseudonymised or anonymised social data can be used for the benefit of insured persons.

At the same time, any opening or standardisation of data access and data spaces must be accompanied by robust and effective safeguards. These may include strict purpose limitation, tiered access concepts, pseudonymisation or anonymisation, verification and authorisation procedures, as well as a clear governance structure with defined responsibilities.

Against this background, DSV supports the consolidation of existing provisions into Regulation (EU) 2023/2854 (Data Act) and Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) in order to enhance legal certainty and implementability.

Furthermore, DSV welcomes the initiative to support the implementation of the Data Act through guidelines on model contractual clauses for data access and data use as well as standard contractual clauses for cloud computing contracts (Article 19 Data Act). Such model contractual clauses are important for social security institutions with regard to cooperation with research institutions and clinics, especially in the field of rehabilitation data.

With regard to data protection impact assessments (Article 35 GDPR), DSV also welcomes the proposed changes according to which the European Data Protection Board will establish uniform lists of processing operations for which a data protection impact assessment is required or not required and will develop a common methodology and a standard template for conducting such assessments.

The proposed modernisation of cookie rules (Articles 88a and 88b GDPR) is also assessed positively. Users should be enabled to give their consent with a single click and to store their cookie preferences centrally in the settings of their browser or operating system. This contributes to legal clarity regarding lawful access to and processing of data, reduces administrative burdens for companies and data subjects, and ultimately improves the user-friendliness of digital services – for example web-based platforms in the field of rehabilitation or aftercare.

With regard to the proposed handling of personal data breaches (Article 33 GDPR), DSV supports the introduction of a single-entry point for reporting breaches at the European Union Agency for Cybersecurity (ENISA). In Germany, there has long been a need to streamline reporting structures, most recently addressed through the ongoing legislative process to repeal Section 83a of Book X of the Social Code, which provides for an additional notification of personal data breaches involving social data to the Federal Office for Social Security (BAS). According to the proposal, the single-entry point would also apply to other reportable incidents under various legal acts, including in the fields of cybersecurity and electronic identification. This can help reduce the administrative burden on public authorities, avoid duplicate reporting and ensure a clear, uniform reporting process. From the perspective of DSV, ENISA is also the appropriate authority for this purpose. At the same time, it must be taken into account that data protection supervision in Germany follows a federal structure and can therefore only be harmonised to a limited extent by EU legislation. In this context, clarification is needed as to how the central reporting point will cooperate with the competent national supervisory authorities.

The proposed extension of the notification deadline under the GDPR is also welcome, as the current 72-hour timeframe is often insufficient to reconstruct the incident and provide a sound basis for risk assessment. It should be clarified whether weekends and public holidays are excluded. From the perspective of DSV, it should also be examined to what extent the proposed extension of deadlines can be aligned with reporting obligations under other EU legal acts – in particular Directive (EU) 2022/2555 (NIS 2 Directive) and Directive (EU) 2022/2557 (CER Directive). A more coordinated approach to deadlines would ease implementation and meaningfully complement the intended simplification through the central reporting hub.

With regard to further proposed amendments to the GDPR, DSV emphasises that any changes must comply with Article 8 of the Charter of Fundamental Rights of the European Union. The issues arising – for example with regard to the definition of personal data (Articles 4 and 41a GDPR), the legal bases for processing with AI (Articles 6 and 9 GDPR), and the scope of data subjects' rights (Articles 33 and 34

GDPR) – must be clarified in close cooperation with the European Data Protection Board.

In particular, DSV urges caution with regard to the processing of special categories of personal data with AI (Article 9 GDPR). The proposed new Article 9(2)(k) GDPR introduces a legal basis intended to regulate such processing. However, this would be linked to the technology used rather than – as currently – to the purpose of processing. This would imply that the processing of sensitive health data using conventional technologies, such as databases, would be prohibited, while it would be permitted when using AI. This would depart from the technology-neutral approach of the GDPR, even though AI-based processing is already possible today for lawful purposes. DSV therefore rejects the proposed provision of Article 9(2)(k) GDPR in its current form.

Irrespective of the individual amendments proposed, DSV emphasises that, with regard to the practical implementation of GDPR requirements in the context of social security, further development of the concept of data protection responsibility is of particular importance. Companies providing IT services and processing personal data should be more strongly obliged to incorporate data protection principles already at the design stage of their services. This applies in particular to processors, who should design their services in a data protection-compliant manner from the outset.

3 _ Electronic identification

DSV supports the objective of establishing, through the European Digital Identity (EUDI) and the EUDI Wallet, the basis for secure, interoperable and cross-border identification procedures. However, it is essential that European solutions are compatible with existing infrastructures in order to avoid duplicate structures and unnecessary interface developments. This also applies with regard to the European Business Wallet (EBW).

In this context, the swift and coherent implementation of the European Digital Identity framework (Regulation (EU) 2024/1183 – eIDAS Regulation) is crucial. It must be ensured that, in addition to the primary identity, supplementary attestations are governed by uniform European standards in order to guarantee their interoperability. It should also be ensured that changes to personal data, such as changes of name or gender, are automatically updated across all relevant attestations in order to avoid national stand-alone processes and to strengthen cross-border interoperability. Overall, existing national legal frameworks as well as established procedures of the

social security system should be taken into account in order to avoid disproportionate administrative or organisational burdens.

Authentication itself should follow clear principles. DSV welcomes that the eIDAS Regulation provides for the principle of data minimisation in this context. Accordingly, relying parties must define in advance which identification data are required for a given purpose and may only retrieve and process those data from the identification means. In addition, it should be ensured that, alongside the standard method of electronic identification, other secure methods remain available so that users can flexibly choose the option that best suits their needs.

About us

The German Federal Pension Insurance (DRV Bund), the German Social Accident Insurance (DGUV), the National Association of Statutory Health Insurance Funds (GKV-Spitzenverband), the national associations for statutory health and long-term care insurance funds at the federal level and the Social Insurance for Agriculture, Forestry and Horticulture (SVLFG) have joined forces to form the "German Social Insurance - Working Group Europe" (Deutsche Sozialversicherung Arbeitsgemeinschaft Europa e. V.) with a view to their common European policy interests. The association represents the interests of its members vis-à-vis the bodies of the European Union (EU) as well as other European institutions and advises the relevant stakeholders in the context of current legislative projects and initiatives. As part of the statutory insurance system in Germany, health and long-term care insurance with 75 million insured persons, pension insurance with 57 million insured persons and accident insurance with more than 70 million insured persons in 5.2 million member companies offer effective protection against the consequences of major risks of life.