Ideas from Stuttgart on modernising data protection

Key points from the perspective of supervisory practice

Unanimously adopted by the independent data protection supervisory authorities of the federal states on 18 June 2026.

Version 1.0, as at 19 June 2026

Abstract

Data protection is firmly enshrined in fundamental rights. It is something the public wants, and local supervision is made extensive use of, particularly by small and medium-sized enterprises and members of the public. Data protection supervision and data protection law both need to be modernised. Competences must be more closely interlinked, and the Data Protection Conference must be enshrined in law. The data protection supervisory authorities of the federal states are putting forward proposals to improve data protection. They advocate the retention of local supervision.

A. Current situation and objectives

Ten years after the adoption of the General Data Protection Regulation (GDPR), a broad debate has developed at both European and national level regarding fundamental reform needs in data protection. This debate concerns not only the interplay between the GDPR and the further legislative acts enacted since 2016 to create the Digital Single Market (the Digital Services Act and the Digital Markets Act, the Data Act and the Regulation on Artificial Intelligence) and their enforcement, but also broader, fundamental questions of innovation and competitiveness, and of safeguarding European values and the ability to act in a globally interconnected, digital world characterised by increasing geopolitical tensions. In Germany, against the backdrop of the implementation of the digital laws and the agreements in the coalition agreement, as well as the federal modernisation agenda, there is also discussion of a reform of data protection supervision.

With these contributions, the data protection supervisory authorities of the federal states are participating in this reform debate. In doing so, they aim to contribute to addressing the reform needs previously identified by academia, politics, business and civil society, drawing on their practical experience to propose recommendations for action which – notwithstanding the time required for the legislative changes that may be necessary in some cases – can be implemented promptly and have a practical impact in the short term.

Core areas of data protection, the protection of privacy and the free movement of personal data, as well as independent supervisory authorities, are protected as fundamental rights at European level under Articles 7 and 8 of the Charter of Fundamental Rights and Article 16 TFEU; they are reserved for the Union legislator and are thus, to a large extent, excluded from national discretion.

Purpose limitation, the balancing of all interests within the framework of a legal basis, consent and the rights of data subjects to intervene constitute the essence of the right to the protection of personal data (Article 8 of the Charter of Fundamental Rights). This means that a concept of 'permission for compatible purposes' cannot be geared solely towards the interests of the data controllers, but must take equal account of the interests of data subjects. Anything else would amount to departing from the framework established by Article 8 of the Charter of Fundamental Rights and lowering the standard of protection afforded by fundamental rights.

Less regulation in data protection, more risk-based regulation or any paradigm shifts cannot be considered in purely national terms. Anyone wishing to change data protection law must convince Europe and comply with the Charter of Fundamental Rights of the European Union. A purely national 'wish list' is not worth discussing!

B. Data Protection Supervision – Myths and Facts

However, in the current debate on reforming data protection supervision, myths are circulating – for example, about allegedly inconsistent data protection supervision or a supposedly excessively strict interpretation by individual supervisory authorities. Against this backdrop, we set out a few facts that shape the framework of data protection supervision ahead of our reform proposals for modernising data protection.

Myth 1: Can data protection supervision be structured however one likes?

The fact is: data protection supervision in a federal system is determined by constitutional law

In the Federal Republic's federal system, data protection in public bodies at state and local authority level can only be monitored by the relevant state authorities. In the areas of healthcare, education and research, schools, culture, the media and the courts, too, legislative competence – and thus also enforcement – lies, in principle, with the states under constitutional law. Supervision without state supervisory authorities is therefore not possible. It also avoids unnecessary overlaps

within a single state. Irrespective of any decision regarding supervisory responsibilities in the non-public sector, data protection supervision in a federal state therefore always involves federal and state authorities, which are subject to the coordination and consistency requirements of the GDPR. Data protection supervision in a federal system is thus, under constitutional law, pluralistic and requires coordination.

Myth 2: Is complaint handling a scalable, high-volume business?

The fact is: over 60,000 complaints – and the trend is rising

In 2025, the federal and state data protection supervisory authorities received well over 60,000 complaints from data subjects; the trend in 2026 is set to rise further, with more than 50 per cent of these originating from the private sector. Despite differences in population figures, the volume of each individual complaint – as a report of a suspected data protection breach – even exceeds the caseload of the Irish authorities responsible for the majority of Big Tech companies operating across the EU.

The call for a fundamental shift in perspective in favour of promoting innovation and data use should not obscure this real need for state enforcement and the fulfilment of the GDPR's promise of protection. Shifts in jurisdiction offer no remedy in this regard and thus ultimately require a one-to-one transfer of staff and costs. Unlike, for example, grant award decisions with clearly defined sets of requirements, data protection complaints offer little potential for structural synergies, as each case requires the examination of individual legal protection concerns, which, at best, allow for only partial categorisation.

The fact is: supervision in the handling of complaints does not scale

The handling of complaints takes up a very large proportion of the data protection supervisory authority's work. The supervisory authority expends considerable resources on making many individual decisions on individual complaint cases. Consequently, the data protection supervisory authority is less frequently visible to data controllers through systematic scrutiny and advice, but primarily through the handling of individual cases. In order to allocate supervisory resources in a more risk-based manner and to achieve even greater standardisation in supervisory practice, legislative amendments are required.

Myth 3: Does centralisation lead to efficiency gains?

The fact is: advice and support are close at hand

In 2025, the state supervisory authorities organised hundreds of events and provided thousands of individual consultations on request at local level. As a result, small and medium-sized enterprises in particular, as well as self-employed individuals – accounting for no less than 99.2 per cent of businesses in Germany – benefit from the current data protection structures. The state data protection authorities provide tried-and-tested local points of contact who are well known through events across the state and regional publications. Local accessibility requires decentralised structures.

The fact is: handling data protection complaints ties up staff

The vast majority of the above-mentioned complaints relate to the business sector. Anyone considering the consolidation or centralisation of data protection supervision will have to take into account that these complaints cannot be dealt with centrally without implications for staffing or costs. Staff cuts lead to reduced protection of fundamental rights.

Myth 4: Is data protection interpreted particularly strictly in Germany?

Fact: There is no ‘German vote’

The German supervisory authorities work together with the other European data protection supervisory authorities within the European Data Protection Board. They have agreed on a wide range of guidelines and other instruments designed to ensure the uniform enforcement of data protection law across the EU. Established and tried-and-tested procedures within the DSK already ensure that there is no so-called ‘German vote’ in the deliberations of the federal and state data protection authorities. The DSK is able to coordinate substantive discussions involving all 18 authorities at very short notice (sometimes within 24 hours), thereby effectively influencing the debate at European level. Cross-border cases are decided in cooperation with other European supervisory authorities or, where necessary, through the consistency procedure within the European Data Protection Board. Sanction proceedings and the levels of fines must also be coordinated at European level in these cases. These procedures set uniform standards across Europe and Germany for supervisory practice, which naturally also have an impact on non-cross-border proceedings. There is therefore no such thing as ‘German data protection’ in the supervisory context.

The fact is: the ECJ upholds the decisions of the German supervisory authorities

There is no overly strict over-interpretation of the GDPR by the German data protection supervisory authorities that would have required correction by the ECJ. In the few decisions of the ECJ that have so far dealt with supervisory measures from Germany, the Court has predominantly interpreted data protection law more strictly than had previously been assessed or practised by the German supervisory authorities.

These include, for example, the retention period for data relating to the discharge of residual debt and the classification of the Schufa score as an automated individual decision under certain conditions.

Myth 5: ‘Inconsistency’ in data protection supervision?

The fact is: coordination mechanisms work

The narrative of inconsistent data protection supervision in Germany is being used, without scrutiny, as a pretext for modernising data protection supervision – a narrative that does not stand up to the current enforcement practice of structurally coordinated cooperation within the Data Protection Conference. Tangible gains in efficiency and legal certainty can be achieved through the

further development of existing and tried-and-tested coordination mechanisms, not through unilateral shifts in responsibilities.

The fact is: diverse data processing activities

The cases dealt with by the German data protection supervisory authorities are as diverse as life itself. The fact that this can lead to differing decisions by the supervisory authorities is not unique to data protection law. More than in any other area of law, the data protection supervisory authorities coordinate their actions in order to reach comparable decisions in comparable cases. To this end, the DSK has agreed on a wide range of guidelines and resolutions designed to ensure the uniform enforcement of data protection law. The small number of decisions handed down by the Federal Administrative Court underscores the broad consistency in the decision-making practice of the German data protection supervisory authorities.

The fact is: binding administrative practice and specific features of state legislation

The supervisory authorities within the DSK recognise the decisions reached by a majority and base their supervisory practice on them. Supervisory authorities with serious concerns may opt out of this self-binding commitment by casting an explicit and reasoned vote. In the vast majority of cases, the DSK aligns its practice with the joint decisions reached; any deviations are, to a not inconsiderable extent, also due to specific features of state legislation.

C. Modernisation of data protection supervision

Coordinated. Efficient. Future-proof.

Data protection rules are currently the subject of intense debate in Germany. Particular attention should be paid to Bundesrat Initiative 356/26 from the Free and Hanseatic City of Hamburg, which aims to make data protection more uniform and efficient for businesses, research institutions and citizens. The DSK supports the proposals and contributes the following aspects – some of which go beyond the initiative – to the discussion:

1. Strengthen the integration of responsibilities. Harness synergies.

The Federal Government’s coalition agreement provides for a ‘consolidation of responsibilities and competences’ among data protection authorities ‘in the interests of the economy’ (line 2106 et seq.). However, the various economic stakeholders are far from unanimous on what the future supervisory structure should look like. The business community is rightly interested in legal certainty and less bureaucracy. This is also a goal pursued by the DSK.

According to a recent survey by the Data Protection Foundation, 48.1% of C-level decision-makers in the private sector (e.g. CEO, CFO or COO) consider a high standard of data protection to be (very) important as a location factor within the EU. As a marker of quality and competitiveness, data protection can be of crucial competitive significance. A trusting, stable and cooperative relationship between businesses and their supervisory authorities is a fundamental prerequisite for this.

The supervisory authorities in the federal states possess detailed knowledge of regional economic and social structures, as well as established networks with businesses – particularly SMEs – as well as trade associations and public administrations. A federally structured data protection supervisory framework enables tailored advice and practical solutions that take into account local specificities and diverse needs.

Centralisation may promise efficiency and uniformity, but it carries the risk of crowding out regional and economic expertise from the federal states. The federal supervisory structure guarantees data protection supervision conducted with due care, which takes regional particularities into account appropriately.

Sustainable improvements and synergy effects can – in line with the objectives of the coalition agreement – best be achieved by pooling competences within the framework of cooperative federalism. Pooling in this sense also means making existing knowledge easily accessible to citizens, businesses, public authorities and supervisory bodies (see point 8).

2. Anchoring the DSK in law

Institutionalise the DSK.

The DSK forms an essential basis for the modernisation of data protection supervision: the Conference of Independent Data Protection Supervisory Authorities of the Federal Government and the Länder has established itself in recent years as the central coordinating body for German data protection supervision. It already plays a key role in coordinating between the Länder and the Federal Government and contributes significantly to the standardisation of the application of the law. Nevertheless, its activities have so far been conducted predominantly on an informal basis, which limits its structural capabilities.

Anchoring the DSK in the Federal Data Protection Act (BDSG) would institutionally secure its role and strengthen its operational capacity in the long term. Clear responsibilities, procedures and objectives should be defined in the BDSG. This would not only increase transparency but also make cooperation more binding.

Experience shows that a uniform interpretation of data protection law can also be achieved through effective and binding coordination mechanisms, without sacrificing the advantages of regional supervision (see point 3).

3. Establishing binding majority decisions

Consistency through binding decisions.

In public debate, German supervisory authorities are frequently accused of applying data protection law inconsistently. It is claimed that this leads to contradictory requirements, which create legal uncertainty and hinder investment. This is incorrect. The introduction of binding majority decisions by the Data Protection Conference (DSK) on matters regulated uniformly across Germany would also dispel these concerns.

The DSK's rules of procedure already provide for such mechanisms, which have proved their worth in practice and have already standardised supervisory practice. In future, these decision-making mechanisms are to be binding on the German supervisory authorities. Binding majority decisions make it possible to clarify outstanding legal issues, take a stance and ensure the uniform application of the law. They provide legal certainty in the application of data protection regulations and are thus a prerequisite for data protection law that promotes innovation.

4. Professionalising the DSK through a secretariat

Strengthening coordination structurally.

At present, the organisation of the DSK's consultation processes, meetings and circular procedures changes with each new DSK chairmanship. In practice, this means that every year a new team of staff from the country holding the chairmanship has to familiarise itself with the tasks and activities associated with the DSK. This makes sustainable knowledge-building, process optimisation and efficient management considerably more difficult. A central DSK secretariat would remedy this situation. The DSK secretariat would then play a key role, as it could ensure organisational and technical support for cooperation between the supervisory authorities and, in particular, improve the preparation, implementation and follow-up of consultation processes. Furthermore, the DSK secretariat could help to systematically document knowledge and make it easily accessible to members of the public, businesses and public authorities. A DSK secretariat ensures continuity and avoids duplication of effort.

5. Targeted pooling of specialist expertise

Concentrating expertise to avoid duplicate structures.

Advancing digitalisation presents data protection authorities with complex and multi-layered challenges, for example in areas such as artificial intelligence, the platform economy, cloud infrastructures, or science and research.

An organisation based on the division of labour within data protection supervision is therefore to be welcomed and is already standard practice today. Through the targeted pooling of specialist expertise, resources can be used efficiently and areas of expertise can be developed.

The pooling of expertise at the BfDI should be achieved by assigning it, in the non-public sector, responsibility for

- ‘market-related cases’ under Article 3(2) of the GDPR,
- advising providers of data processing services of an infrastructural nature serving many users within the federal territory,
- the central coordination of codes of conduct and the accreditation of certification bodies, as well as
- representation in technical standardisation

procedures.

6. Providing guidance, particularly for businesses,

provide clarity for practical application.

The General Data Protection Regulation (GDPR) contains a large number of general clauses and open-ended legal terms. Clear and practical guidance is therefore crucial.

Joint positions adopted by the DSK enable organisations in particular to better understand and implement data protection requirements. At the same time, they support the supervisory authorities in applying the law consistently. Consequently, the supervisory authorities have, in the past, regularly and unanimously published a wealth of guidelines, practical advice and guidance. In line with the Helsinki guidelines, dialogue and practical guidance are to be further expanded in future.

7. Central digital portal (single entry point & ‘no wrong door’)

Simplifying access.

The establishment of a unified digital access point to data protection supervision in the non-public sector is a key component of a modern and user-friendly administration. In line with the ‘no wrong door’ principle, it should in future be possible to receive all enquiries via a central digital portal, regardless of the data protection authority’s jurisdiction (in terms of subject matter and geographical area). In addition, the reporting channels for data breaches are to be centralised. Subsequent forwarding and processing will take place efficiently and seamlessly. This will simplify access to data protection supervision whilst simultaneously speeding up the handling of enquiries. It will also create a clear and uniform communication channel for companies with multiple sites.

A central digital portal enhances the efficiency of supervision without abandoning the federal structure. It is a prerequisite for modern, user-friendly administration.

8. Establish a shared decision-making database

Increasing transparency and consistency.

Decisions by the German data protection supervisory authorities have not, to date, been systematically collated and published. A joint database for data protection supervision, containing decisions and publications such as guidance notes and handbooks, could remedy this situation if a secretariat of the DSK were to support such work (see C.4. above) and if statutory authorisation for publication were established in the area of administrative fines. This would enable citizens and businesses to better understand supervisory practice, leading to greater reliability and predictability.

The DSK is therefore currently developing a concept for a joint decision database. In the long term, this will create greater transparency, increase legal certainty for all parties involved and make a further contribution to the uniform application of the GDPR, as it will facilitate access to existing knowledge and enable decision-making practices to be harmonised.

9. Introducing the ‘one-for-all’ principle

Avoiding duplication of effort.

A major efficiency issue with the current supervisory structure in the non-public sector lies in parallel investigations into similar or identical matters by several authorities. This leads to increased administrative burdens for all parties. The ‘one-for-all’ principle addresses precisely this issue.

It provides that the examination of a matter by a competent supervisory authority is binding nationwide, provided that this matter is regulated uniformly by law across the country. This ensures that identical issues do not have to be examined multiple times. Significant efficiency gains can be achieved in this way, particularly in the case of complex, cross-state matters.

At the same time, the principle contributes to the standardisation of the application of the law, as an assessment made once applies to all parties involved. The DSK is therefore currently working on the development of standards and templates to help those responsible fulfil their documentation obligations. The use of these standards and templates leads to improved quality and comparability of the documentation and is an important prerequisite for the cross-border recognition of audit results.

10. Strengthening coordination and speeding up procedures

Efficiency through clear processes.

Improving coordination is a key starting point for reforms. The aim is to standardise procedures, harmonise assessment criteria and speed up decision-making processes without compromising the quality of the application of the law.

A key element in this is the introduction of clear processes and responsibilities. Single points of contact, for example in the form of a ‘one-stop shop’ model, can significantly simplify communication.

Improved coordination (see point 4) makes it possible to retain the advantages of the federal structure whilst significantly increasing efficiency: modern data protection supervision is achieved not through centralisation, but through optimised cooperation on a federal basis.

D. Key propositions on substantive data protection law

Modernising data protection law in a targeted manner

The Data Protection Conference has put forward a series of concrete proposals for the further development of substantive data protection law, for example regarding the protection of children online or the promotion of research in the public interest. Furthermore, the General Data Protection Regulation could and should be modernised in several respects.

1. Guidelines for AI

The use of AI requires a secure framework. Alongside the guidelines already under discussion for the appropriate training of AI using personal data, effective enforcement of data subjects’ rights must be ensured. When using AI systems, technical, organisational and legal safeguards must ensure the effective implementation of the fundamental principles of data protection.

2. Improving Operationalisation

A number of regulations should be streamlined to improve their functionality and operationalisation. Instruments of self-regulation – particularly those within the business sector – which have so far been dysfunctional need to be simplified. This applies in particular to certification and codes of conduct (Art. 40 et seq. GDPR).

3. Examining risk-based approaches

Some risk-based approaches can be incorporated into the GDPR, but with caution. Examples might include the processing of special categories of data (Article 9 of the GDPR) or the transfer of data to third countries (Article 44 et seq. of the GDPR). This may lead to simplifications in some data processing operations, but also to stricter requirements in others.

4. Reducing red tape in data processing, holding manufacturers accountable

The legal framework for data processing relationships offers considerable potential for simplification without compromising data protection: by restructuring data processing into a statutory contractual relationship, unnecessary verification requirements and sources of error can be reduced. At the same time, data processing based on a division of labour is simplified and made less bureaucratic. Above all, to ease the burden on SMEs, the obligations of those involved in data processing must be distributed more fairly. Application manufacturers must be held accountable for their products and solutions under the GDPR, following the model set out in the AI Regulation.

5. Strengthening the protection of fundamental rights

Data protection law could be geared more strongly towards maximising societal benefits without weakening the protection of fundamental rights. The focus should be on high-risk data processing operations. To this end, it should be possible to prioritise the handling of complaints, not least to create scope for targeted support for innovative and data-protection-compliant applications. Whatever changes are made to the GDPR, the protection of personal data under Article 8 of the Charter of Fundamental Rights, Article 16 of the TFEU and the general principles of Article 5 of the GDPR must be upheld.