



# Position Paper

of the German Bar Association prepared by the  
Committee on IT Law

on the Proposal of the European Commission  
for a Digital Omnibus Regulation (COM (2025)  
837 final)

Position Paper No.: 21/2026

Berlin/Brussels, March 2026

## **Members of the IT Law Committee**

- Rechtsanwalt Prof Niko Härting, Berlin (chair, rapporteur)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main (rapporteur)
- Rechtsanwältin Dr. Christiane Bierehoven, Düsseldorf (rapporteur)
- Rechtsanwältin Isabell Conrad, München (rapporteur)
- Rechtsanwalt Prof. Dr. Malte Grützmaker, LL.M., Hamburg (rapporteur)
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf (rapporteur)
- Rechtsanwalt Dr. Helmut Redeker, Bonn (rapporteur)
- Rechtsanwältin Dr. Kristina Schreiber, Köln (rapporteur)
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (rapporteur)

## **In charge in the Berlin Office**

- Rechtsanwältin Nicole Narewski, Director, Berlin

## **Contact in Brussels**

- Rechtsanwältin Eva Schriever, LL.M., Director
- Rechtsanwältin Dorothee Wildt, LL.M., Deputy Head of Office
- Myra Jockisch, LL.M., Legal Advisor

**Deutscher Anwaltverein**  
Littenstraße 11, 10179 Berlin  
Tel.: +49 30 726152-0  
Fax: +49 30 726152-190  
E-Mail: [dav@anwaltverein.de](mailto:dav@anwaltverein.de)

**Büro Brüssel**  
Rue Joseph II 40, Boîte 7B  
1000 Brüssel, Belgien  
Tel.: +32 2 28028-12  
Fax: +32 2 28028-13  
E-Mail: [bruessel@eu.anwaltverein.de](mailto:bruessel@eu.anwaltverein.de)  
EU-Transparency Register ID number:  
87980341522-66

The German Bar Association (Deutscher Anwaltverein – DAV) is the professional body comprising about 60.000 German lawyers and lawyer-notaries in 253 local bar associations in Germany and abroad. Being politically independent the DAV represents and promotes the professional and economic interests of the German legal profession on German, European and international level. The DAV is registered in the Lobby Registry for the representation of special interests vis-à-vis the German Bundestag and the Federal Government under register number R000952.

---

The German Bar Association (Deutscher Anwaltverein, DAV) hereby comments on the Regulation 2025/0360 (COD) from the EU Commission's draft COM (2025) 837 final in its version dated November 19, 2025.

**a) Executive summary**

The implementation of the requirements of the GDPR, the Data Act, the AI Act, and other data law instruments is not always easy in practice. The DAV therefore welcomes the attempt to clarify some of the existing uncertainties and provide greater legal certainty through two “omnibus packages.” This is beneficial for the rights of citizens, for the companies and institutions concerned, and for the authorities responsible for enforcing these legal acts.

In principle, the DAV also particularly welcomes the attempt to address the specific data protection issues that arise when personal data is used for the training and operation of AI applications by amending Article 9 GDPR and introducing a new Article 88c GDPR. A separate Position Paper is intended to address the details.

- Rights of access: The DAV welcomes modifications to the data protection rights of access. Rights of access are a central instrument for realizing the data protection rights of citizens. These rights must neither be misused nor undermined through abusive requests. Introducing an obligation to provide reasons for access requests could be helpful, since without such justification it will often be difficult to assess whether a request is abusive.

- Notification obligations: The DAV welcomes modifications to the notification obligations. Excessive reporting of data breaches that authorities are unable to process thoroughly benefits no one. One must support the goal of establishing a single reporting authority and a uniform reporting channel for breach notifications under different legal acts.
- Additional provisions: The proposals for supplementary rules concerning research data, biometric data, and automated individual decision-making also deserve support, notwithstanding some criticism regarding the details.
- Cookies: In addition to the protection of personal data, under current technical conditions there is no longer a separate need to protect end-user devices from cookies. The DAV therefore welcomes the planned transfer of the long-debated data protection provisions on “cookies” from the ePrivacy Directive into the GDPR. This transfer should be accompanied by the complete deletion of the “cookie” provisions from the ePrivacy Directive.
- Personal data: The DAV does not see a compelling need to adapt the concept of personal data in the GDPR to more recent case law of the CJEU. However, if such an adjustment were to take place, it should be clarified more explicitly whether and to what extent the case law of the CJEU is intended to be modified.
- Pseudonymization: The DAV welcomes additional rules on pseudonymization but suggests complementing them with provisions on anonymization. Pseudonymization and anonymization are important practical instruments of data protection and should be strengthened.
- Data Code: The DAV welcomes the effort to simplify the Data Act and expand it into a comprehensive data code. However, it considers that the proposals in the “omnibus” package still require significant alterations.

**b) Changes to the rights of data subjects**

The aim of the proposed amendments to Articles 12, 13, and 22 of the GDPR is to achieve a better balance and improve the practical reconciliation between the fundamental rights and freedoms of individuals who are entitled to data subject rights and the respective controller. This objective is to be welcomed. The considerable

practical need for such improvements is particularly evident in the context of employment relationships and in the field of artificial intelligence.

The planned amendments to Articles 12, 13, and 22 GDPR, as well as the drafts of new recitals (35) to (38), contain promising approaches. However, they could be further refined by avoiding the introduction of terms that themselves require clarification and could lead to new legal uncertainty.

## **1. Amendments to Article 12(5) GDPR**

The Commission's proposed amendment to Article 12(5) of the GDPR provides that:

*“Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character or also, for requests under Article 15 because the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data, the controller may either:*

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or*
- (b) refuse to act on the request.*

*The controller shall bear the burden of demonstrating that the request is manifestly unfounded or that there are reasonable grounds to believe that it is excessive.”*

## **2. Proposal to clarify the concept of "abusive"**

The relationship between “abusive” and “unfounded” or “excessive” is not clear. Therefore, it should be considered to include a clarification in Art. 12(5) GDPR, for example by introducing the word “such as”:

*“such as where the data subject abuses the rights granted to them by this Regulation for purposes other than the protection of their data ...”*

As far as the draft recital (35) mentions, by way of example, that “[o]verly broad and undifferentiated requests for information [...] should also be considered excessive,” this is to be welcomed, as it is indeed a situation that occurs frequently in practice.

However, the example should be specified, because not every nonspecific request for information is excessive or abusive, particularly when the data have not been collected directly from the data subject.

### **3. Proposal for an obligation to provide reasons for requests for information**

In order for the amendments to Art. 12(5) GDPR not to be ineffective, a requirement should be established in relation to Art. 15 GDPR for data subjects to provide a justification, so that the controller can assess whether the data subject has abusive intentions. Such a justification requirement can also facilitate a dialogue between the controller and the requester in cases of nonspecific information requests, allowing for clarification of the information and copies to be provided.

A justification requirement appears necessary to enable the controller to assess the potential abusiveness of a request for information. Without such a requirement, the proposed amendments to Art. 12(5) GDPR could be rendered ineffective.

According to the current recital 63 GDPR, the right of access exists to allow the data subject “easily and at reasonable intervals” to “become aware of the processing of data” and “verify its lawfulness.” According to the CJEU (Judgment of 26 October 2023 – C-307/22, *Patientenakte*), this is possible without providing reasons.

Under the draft amendment to Art. 12(5) GDPR, a request for information is considered abusive if it is made “for purposes other than the protection of the data.” This gives rise to several practical difficulties in implementation:

- How can the controller assess whether the request is made solely for the protection of data if the data subject is not required to provide reasons for the request?

- Does the data subject's intention to lodge a complaint under Art. 77 GDPR and/or claim damages under Art. 82 GDPR in the event of unlawful processing revealed by the information request, or in the case of refusal or manifestly incorrect fulfillment of data subject rights, already render the request abusive? Or are all such cases encompassed by the purpose of "protection of the data"?
- Data subjects often have multiple motives for an information request, partly to exercise their GDPR rights and partly for other purposes. Does annoyance over marketing communications and verification of compliance with § 7 of the German Act against Unfair Competition, or an ongoing unfair dismissal proceeding by the data subject against the controller, render a situationally submitted request abusive?
- Does the fact that, in the context of litigation, some of the creditor's claims—including a request under Art. 15 GDPR—have not yet been fulfilled, and the creditor offers a settlement with full resolution, per se render the information request abusive?
- The examples in the draft recital (35) suggest that the data subject's intentions are relevant, for instance, if the request is made "solely with the intention of causing harm to the controller." But how is such a "sole intention" to be proven for the controller, even if the burden of proof is limited to "sufficient reasons to assume" excessiveness?
- The purpose pursued by the requester can also change. In practice, a dialogue often takes place between controller and requester during the provision of information. For example, the data subject may initially submit a nonspecific request to become aware of the processing (recital 63 GDPR), and after receiving an initial response from the controller, which may not be sufficiently transparent, the data subject may send follow-up requests pursuing other purposes (e.g., asserting claims for damages due to misinformation, for which the initial disclosure provides evidence). To what extent does this constitute an abuse of the right of access under the draft amendment to Art. 12(5) GDPR?
- Does the fact that, in the context of litigation, some of the creditor's claims—including a request under Art. 15 GDPR—have not yet been fulfilled, and the creditor offers a settlement with full resolution, per se render the information request abusive?

#### **4. Proposal to restrict Art. 15(3) GDPR**

In Art. 15(3) GDPR, the frequent case should be explicitly addressed in which an employee or former employee with many years of service at the controller's establishment or office (including legal representatives and senior management such as shareholders, board members, managing directors, etc.) submits a nonspecific request for access that encompasses a large volume of data, most of which they themselves created (e.g., e-mail communications). In such cases, the controller should be able to require the specification of the request and refuse to provide copies if no specification is made, unless there are legitimate reasons on the part of the data subject why specification is not possible or reasonable.

While information requests made with abusive intent should be entirely denied, in the case of "overly broad and undifferentiated requests for access," it may be necessary to differentiate between the information pursuant to Art. 15(1) and (2) GDPR and the burdensome right to obtain copies under Art. 15(3) GDPR.

According to the case law of the CJEU (most recently in Judgment of 4 September 2025 – C-413/23 P, SRB), messages or statements are generally considered personal data of their author in their entirety. Since an employee's e-mails typically also concern the rights of other persons to a significant extent (personal data of third parties, and potentially business secrets, Art. 15(4) GDPR), the controller faces enormous efforts in producing copies and carrying out redactions, particularly where the former employee has long-standing service.

When redacted copies of e-mails are provided to an (former) employee requesting access, they can often reconstruct information using their additional knowledge—for example, the identities of other persons whose names were redacted. This raises the question to what extent copies of e-mails can be withheld in whole or in part under Art. 15(4) GDPR, which the controller currently has to assess on a case-by-case basis for each individual e-mail.

Digital redaction of unstructured data such as e-mails is rarely reliably automated and also carries a significant risk that redacted information can be reconstructed. In recent years, this risk has increased substantially due to AI-supported analytical tools, which can partially or fully reconstruct redacted passages. This risk cannot be completely mitigated even by printing and rescanning (roundtripping), at least not for large volumes of data. In addition, the additional effort involved in scanning and quality control for large volumes of redacted printouts is considerable, on top of the effort required for digital redaction. Consequently, Art. 15(4) GDPR does not prevent disproportionately high burdens for the controller in the case of nonspecific access requests, and such burdens often do not even lead to the desired legal certainty.

## **5. Need for clarification regarding email copies in the employment context**

Article 15(3) GDPR should also be amended to require the applicant to specify and limit their request for copies, and to clarify that the controller may decide whether to provide the copies electronically or by other means, taking into account data security, where the information concerns an employment relationship of at least 12 months and comprises large volumes of the applicant's work-related e-mails.

In practice, a recurring question arises as to whether, in the case of electronic transmission of large volumes of (partially redacted) work-related e-mails to the data subject, the data remains sufficiently secure with respect to its retention on the data subject's systems. While the controller must ensure the security of the transmission channel, no standard or defined level of security exists for data stored on the data subject's IT systems, which are typically private.

This raises the question of whether the (former) employee should always have the right to request electronic delivery of an (unspecified) copy (Art. 15(3), third sentence GDPR), or whether the controller may, under certain circumstances, refuse to transmit large volumes of redacted e-mails electronically—at least where the data subject has not specified the request—and instead fulfill the request by providing a paper copy.

## **6. Changes in draft Art. 13 GDPR and relevance for Art. 14 and 15 GDPR**

The proposed amendments to draft Art. 13(4) GDPR are unlikely to provide significant relief for larger controllers, because Art. 13 is generally easier to comply with compared to Arts. 14 and 15 GDPR. For smaller entities, such as local associations or craft businesses, which have previously been overwhelmed by the overall requirements of data protection information, the amendments could offer some relief. As a result, the proposed changes are to be welcomed.

## **7. Proposal for clarifications in draft Articles 13 and 14 GDPR**

The terms “not-data-intensive activity” and “clear and circumscribed relationship” need to be further specified, as otherwise legal uncertainty and divergent interpretations are to be expected.

The vague terms are somewhat clarified by the examples in the corresponding draft recital (36), but they are not used consistently. It states: “where the context of the relationship between the controller and the data subject is very clear and circumscribed and the controller’s activity is not data intensive [...]”, suggesting that “not-data-intensive” refers to the nature of the processing, but not its complexity.

Recital (36) continues: “The controller’s activity is not data-intensive where it collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.” According to this, the quantity of data and the scope of processing appear decisive for “not-data-intensive.” Why data processing in the employment context is considered small-scale and not complex is not immediately apparent, given practices such as e-recruiting or employee background checks, unless one restricts the reference to small associations or micro-enterprises.

It would be particularly desirable, especially for associations and micro-enterprises, for recital (36) to clarify that the amendment to draft Art. 13(4) GDPR can also cover privacy statements on websites, provided that no cookies or other tracking mechanisms

are used. Without such clarification, new waves of warnings could arise regarding missing privacy information on websites.

Furthermore, with regard to the CJEU judgment of 4 September 2025 (C-413/23 P, SRB), it should be clarified that the exception in draft Art. 13(4) GDPR may also apply where the controller pseudonymizes data in an anonymizing manner and only discloses it in that form to recipients.

Facilitation for scientific research is generally desirable. However, in the draft Art. 13(5) GDPR, a problem similar to that in Art. 14(5)(b) GDPR arises, namely that in practice there is considerable legal uncertainty as to when disproportionate effort is involved. The example in recital (37) of a change of purpose for research purposes, which could not have been anticipated at the time of collection, is helpful.

It should, however, be clarified that this scenario also applies under Art. 14(5)(b) GDPR. In addition, the relationship to the disproportionate effort for access requests under Art. 15 GDPR should be clarified.

It seems somewhat imbalanced that proportionality considerations have been sharpened for both Art. 13 (information obligation for direct collection) and draft Art. 12(5) GDPR (access), but not in Art. 14 GDPR, which often represents the greatest practical difficulty, especially for training AI systems, as well as for RAG systems. The data used for this (e.g., documents with author names in knowledge bases of RAG systems) is often freely accessible online, i.e., from publicly available sources.

Where the processing of data from publicly available sources is not likely to result in a high risk to data subjects—particularly if the data were made public by the data subjects themselves—and where providing information would be disproportionate due to the number of data subjects and uncertain e-mail contact possibilities, the information obligation under Art. 14 GDPR should be capable of being fulfilled through a publication (e.g., online job postings).

### III. Automated individual decision-making, research data, and biometric data

#### 1. Automated individual decision-making, Article 22 GDPR

It is urgent, particularly in the context of AI agents and automated workflows, to clarify the term “necessary” in the draft Art. 22(1)(a) GDPR. The distinction from the GDPR-specific term “required” is not evident from the text of the provision itself. The intended meaning only becomes clear from the corresponding recital (38).

It is desirable to embed this clarification in the regulation text:

*“Necessary’ means that the fact that a human could also make the decision does not prevent the controller from making the decision solely by automated processing.*

*Where multiple equally effective automated processing options are available, the controller should use the less intrusive solution.”*

Through the proposed amendment, the previous paragraphs 1 and 2 of draft Art. 22 GDPR have been combined, and the provision has been transformed into a list of lawful bases rather than a right of the data subject. This is understandable; however, the placement in “Chapter III – Rights of the Data Subject” now seems somewhat less appropriate.

The relevance of draft Art. 22 GDPR for AI-supported decision-making processes is very significant. This applies even in cases of non-fully automated processes involving human decision-makers, where AI recommendations substantially influence the decisions, because the human lacks sufficient insight and ability to independently assess the outcome (CJEU, Judgment of 7 December 2023 – C-634/21, SCHUFA). In the scope of application of draft Art. 22 GDPR, the term “legal effect” has been changed in the German draft regulation to “effect of law” (“Rechtswirkung”). No substantive change is intended thereby.

The proposed clarification in the new version of Art. 22(1)(a) GDPR, that in assessing whether a decision for entering into or performing a contract with a data subject is “necessary,” it is not required that the decision could only be made through automated processing, is to be welcomed. Ultimately, this clarification enables easier practical implementation without significantly restricting the relevant rights of data subjects.

## **2. Research data**

The proposal to concretely define the term “scientific research” through the introduction of Art. 4(38) GDPR, and to clarify through the revised Art. 5(1)(b) and the addition of Art. 13(5) GDPR that further processing for scientific purposes is compatible with the original purpose of processing and that scientific research constitutes a legitimate interest, is fundamentally to be welcomed.

In particular, the clarification that research may also serve the promotion of a commercial interest appears reasonable and practical, especially as it ensures a definition consistent with Regulation (EU) 2025/327 on the European Health Data Space. Through these amendments, research and innovation activities serving the public interest—even if data-intensive—are effectively privileged. This objective, especially in view of strengthened innovation promotion, is sensible.

Certainly, this creates a potential for misuse, as companies may declare research activities without any underlying scientific methodology, systematic pursuit of knowledge, or quality-assured procedures. Determining whether misuse has occurred is likely to be difficult and complex due to the various indeterminate legal terms involved.

On the other hand, there is no objection to leaving this assessment to supervisory authorities or the courts, particularly since the potential for misuse has already existed. What appears more important is to strengthen the research privilege and then, in enforcement, ensure that it is only used for actual research projects to the necessary extent.

### 3. Biometric data

The proposal to introduce an exception to the general prohibition on the processing of biometric data by adding Article 9(2)(l) GDPR—where such processing is necessary to verify the identity of the data subject and the data and means for such verification are under the sole control of that person—is fundamentally sensible. However, the reference to the “sole control” of the data subject over the data or means appears too vague. It would be preferable to instead rely on appropriate technical and organizational measures:

*“(l) processing of biometric data is necessary for the purpose of confirming the identity of a data subject (verification), where the biometric data or the means needed for the verification is under the sole control of the data subject.”*

Recital (34) should also be understood in this sense, especially since it explicitly refers to the encryption of biometric data in accordance with the state of the art.

#### c) Reporting obligations

The DAV expressly welcomes the amendments contained in Proposal COM (2025) 837 final regarding the consolidation of reporting obligations through a single point of contact at ENISA. The introduction of the “report once, share many” principle represents a significant step forward in reducing administrative burdens. As the reports may include highly sensitive information concerning the affected entities, the technical, operational, and organizational measures to be taken by ENISA under Article 23a (2) of the proposed amendment to the NIS-2 Directive should not only be “appropriate and proportionate” but also effective and in line with the state of the art.

The DAV considers it essential that ENISA acts as a trustee, with the reporting entity retaining exclusive control over the disclosure of the information. Accordingly, Article 23a (4) of the proposed new provision should generally preclude ENISA’s access to the submitted reports.

Also to be positively noted are the extension of the reporting period under Article 33 GDPR to 96 hours and the raising of the risk threshold in alignment with Article 34 GDPR.

However, the reporting obligations under the NIS2 Directive, DORA, the eIDAS Regulation, and the CER Directive should likewise be alleviated through an extension of the reporting period to ensure a consistent and practicable reporting procedure.

#### **d) Proposed amendments to cookies**

From the DAV's perspective, the amendment to Article 5 of Proposal COM (2025) 837 final does not appear sensible. It risks further complicating the already very complex relationship between the GDPR, the ePrivacy Directive, and the Data Act, thereby increasing both legal uncertainty and compliance burdens for all parties involved. Important innovation-driven sectors, such as the Internet of Things and related initiatives (e.g., Industry 4.0 or connected driving), would be adversely affected.

The DAV therefore recommends, at the very least, refraining from the new provision on the primacy of application of the new Article 88a GDPR currently foreseen in the omnibus Proposal COM (2025) 837 final (see Section VI.1.). In addition, the DAV proposes the complete deletion of Article 5(3) of the ePrivacy Directive (see Section VI.2.).

#### **1. The proposed amendment would only exacerbate existing legal uncertainty**

Even under the current legal framework, companies seeking to build a business model around connected objects and the data generated by them must ensure compliance with at least three different regulatory instruments:

- Data Act
- GDPR
- Article 5(3) of the ePrivacy Directive, and its national implementation.

All three instruments regulate the same subject matter: they set out whether and under what conditions a company may extract data from or upload data to a connected object. These instruments therefore form “regulatory layers” over the same subject matter. A business model can only be implemented if the company complies with the requirements of all three layers. It is evident that each additional layer increases administrative burdens, raises legal risks, and may preclude certain (even legitimate) opportunities to generate revenue.

This is particularly problematic where the regulatory instruments lead to conflicting results. Some of these “problematic areas” in overlapping regulatory frameworks are already difficult for companies to navigate with legal certainty. For example, the relevant provision in the Data Act (Article 4(13)) applies only to non-personal data—even though, from the company’s perspective, it is often legally uncertain whether the data qualify as personal and this classification may change retroactively.

A similar problem would arise under the proposed new subparagraph to Article 5(3) of the ePrivacy Directive, which would establish the primacy of the new Article 88a GDPR. In most cases, it is simply impossible to determine in abstract terms whether a particular business model or process involves personal data. This may change depending on context—for example, if additional knowledge becomes available or if data are shared with third parties (see ECJ case law on SRB, C-413/23 P; OLAF, C-479/22 P; Gesamtverband Automobilteile-Handel, C-319/22). Moreover, the definition of “personal data” is already based on the so-called Breyer test (now Recital 26 GDPR), which considers whether the data subject can be “reasonably likely” to be identified. These are inherently vague legal concepts, requiring case-by-case assessment and often giving rise to divergent legal interpretations in practice.

Innovation-driven sectors require legal certainty—or, at minimum, the ability to implement innovative business models under manageable risks where legal certainty is lacking.

Regulations such as the one proposed here are, figuratively speaking, “poison” for innovation-driven companies: they create legal uncertainty while simultaneously imposing extreme risks—violations of the GDPR or national transpositions of Article

5(3) ePrivacy Directive can trigger fines and class actions of potentially existential magnitude.

The newly proposed subparagraph would place companies in an impossible situation: on the one hand, they would have to predict with certainty how an authority or court would classify the personal nature of processed data in a complex (borderline) case; on the other hand, the draconian legal consequences remain if the company's assessment later proves "incorrect."

Finally, the new subparagraph would create a systematic inconsistency: a provision that does not apply to personal data would impose stricter requirements than a provision that does. This is structurally unsound.

Against this background, the DAV proposes deleting the new subparagraph under Article 5(3) of the ePrivacy Directive.

## **2. Article 5(3) of the ePrivacy Directive should be deleted in its entirety**

Instead of the new subparagraph, Article 5(3) of the ePrivacy Directive should be deleted in its entirety.

The provision was originally (presumably) introduced because, at the time of the ePrivacy Directive's adoption, the EU legislator was confronted for the first time with cookies—small text files placed by website operators on users' devices to store data and retrieve it later. The EU legislator considered this sufficiently problematic to establish a rule making the setting of cookies subject to a prohibition with a prior consent requirement.

Due to the open wording of the provision, it has since taken on a life of its own, beyond what the original legislator intended. It is now applied not only to cookies but to a wide range of other technologies—for example, the Internet of Things mentioned above, as well as all forms of tracking online or via applications. Some legal literature even debates whether the installation of software updates falls within its scope—which, based on the wording, could be affirmed.

According to the DAV, it would be appropriate to reconsider the actual purpose of the provision and whether it achieves that purpose. From the DAV's perspective, the answer is negative.

Article 5(3) ePrivacy Directive, as a privacy-protective provision, has a purpose similar to Article 6 GDPR, but differs in two important respects:

- Unlike Article 6 GDPR, Article 5(3) ePrivacy Directive also applies to non-personal data. Its scope encompasses all data stored on end-user devices. Article 5(3) ePrivacy Directive allows only three possible justifications for storing or accessing such data: for the provision of a service explicitly requested by the user (limited to processing strictly necessary for that service); for the transmission of a communication in a telecommunications network; or with the user's consent.

This combination of a very broad scope with highly restrictive permissions has caused significant negative effects in practice: for many data processing activities, no other legal basis than consent exists. This has, particularly online, led to a flood of consent banners that users perceive as disruptive and routinely "clicked away" without consideration. The intended protective and alert function of consent is thus lost—creating the so-called "consent fatigue."

The design of Article 5(3) also produces regulatory conflicts with other rules and leads to incoherent results. For example, what if a company must access data on a device to fulfil a legal obligation or achieve an important public interest objective (e.g., ensuring cybersecurity)? The GDPR addresses such purposes under Articles 6(1)(c), (d), or (f). Article 5(3) ePrivacy Directive contains no comparable exceptions. Taken literally, it would prohibit data storage or access even for these purposes.

Further inconsistencies arise in relation to the legal bases in Article 6 GDPR. These provisions indicate that certain processing is meant to be allowed by the EU legislator—for instance, when it serves a legitimate interest and does not override the interests of

the data subject (Article 6(1)(f) GDPR). Why should the GDPR permit such processing, while Article 5(3) ePrivacy Directive does not? Both provisions pursue largely the same protective purpose, yet one is considerably stricter than the other.

From a policy perspective, the protective purpose of Article 5(3) ePrivacy Directive is difficult to justify. For “ordinary” data protection, GDPR already provides sufficient safeguards, setting out the conditions under which intrusions into users’ privacy are justified. If the EU legislator deems these protections insufficient, this should be addressed within the GDPR, not through a provision external to the system in the ePrivacy Directive.

To the extent that Article 5(3) ePrivacy might be intended to achieve an economic protective purpose, this would be systemically misplaced and, moreover, already addressed in Article 4(13) Data Act.

Ultimately, the only remaining protective purpose is the safeguarding of a particular form of privacy: the “informational integrity of the end device,” i.e., the user’s control over which information may “enter” or “leave” their device—similar to the constitutional right to the inviolability of one’s home.

However, this purpose is exaggerated and not appropriate from a policy perspective. Communication devices are designed to receive and transmit information; making this subject to a prohibition with a prior consent requirement is innovation-hostile and creates bureaucracy. A meaningful regulation should focus not on the “whether” but on the “how” of data processing. Possible measures include transparency and information obligations, prompts regarding device default settings, or restrictions on certain data collection practices (e.g., profiling). Importantly, such measures should be systematically integrated into the correct legal framework—e.g., GDPR for personal data or the UCP Directive for practices considered unfair.

e) **Definition of personal data**

The approach of aligning the definition of “personal data” in Article 4(1) GDPR with the case law of the CJEU is to be welcomed, as it provides clarity. This clarifies whether, in determining whether data are personal, only the means available to the respective data controller should be considered (a relative notion), or whether it is sufficient that any entity or data processor could establish a personal reference (an absolute notion).

However, the draft does not implement the CJEU case law in all respects.

**1. Problem statement**

**a) The latest case law of the ECJ**

In its SRB judgment of 4 September 2025, the CJEU ruled regarding the personal nature of pseudonymised data that the existence of additional information enabling the identification of data subjects does not mean that pseudonymised data are, in every case and for every person, personal data (CJEU, Judgment of 4 September 2025, C-413/23 P, paras. 82, 86). Rather, depending on the circumstances of the individual case, pseudonymisation can prevent other persons from identifying the data subject, so that the data are not or are no longer personal for those other persons (CJEU, Judgment of 4 September 2025, C-413/23 P, paras. 86 ff.).

Depending on the circumstances of the individual case, the controller who performed the pseudonymisation may have access to additional information enabling the identification of data subjects (CJEU, Judgment of 4 September 2025, C-413/23 P, para. 76). Likewise, a third party to whom the controller has transmitted the data may also possess such means to establish such an identification (CJEU, Judgment of 4 September 2025, C-413/23 P, para. 77).

The same applies, according to the CJEU, where the controller provides pseudonymised data to third parties who possess means that may enable the identification of data subjects. In that case, the data is personal not only for the third

party but also for the controller (“indirectly,” see CJEU, Judgment of 4 September 2025, C-413/23 P, para. 84). According to the CJEU, this rule prevents pseudonymised data, which in themselves have no personal reference but for which such a reference can be established by other persons, from being wrongly excluded from the scope of Union data protection law (CJEU, Judgment of 4 September 2025, C-413/23 P, para. 85).

The CJEU therefore assesses the personal nature of data on a case-by-case basis and determines, for the purpose of assessing identifiability, that the relevant persons are those individuals, entities, or bodies—including recipients of the data—who possess the means to identify a data subject, even in the case of pseudonymised data. It is irrelevant that any arbitrary third party, not involved in the processing and not provided with the data, could establish a personal reference. Accordingly, the CJEU applies a relative assessment of personal data on a case-by-case basis and rejects an absolute approach.

#### **b) Planned amendment to Art. 4 No. 1 GDPR**

The draft amendment to Article 4(1) GDPR deviates in its third sentence from the CJEU case law. According to the case law, data are not considered personal merely because a potential future recipient possesses means that could, with sufficient likelihood, be used to identify the natural person to whom the information relates.

As already explained, the CJEU has held the opposite: pseudonymised data are deemed (“indirectly”) personal for the transmitting entity if a later recipient is able to make such an identification (CJEU, Judgment of 4 September 2025 – C-413/23 P, SRB, para. 84, with reference to Judgment of 9 November 2023 – C-319/22, Gesamtverband Autoteile-Handel, paras. 46 and 49, regarding the personal nature of the VIN when transmitted by a vehicle manufacturer).

According to Recital 27 of the draft proposal, and in line with the relevant CJEU case law on the definition of personal data, it should be clarified in detail when a natural person should be regarded as identifiable. In particular, it should be made clear that information is not considered personal data for a given entity if that entity does not

possess means that could, with sufficient likelihood, identify the natural person to whom the information relates. If such information is subsequently transmitted to third parties who themselves, based on reasonable judgment, possess means to identify the natural person to whom the information relates—for example, by matching it with other data available to them—the information becomes personal data only for those third parties who possess such means. For the reasons set out above, this last sentence of the recital deviates from the CJEU case law.

## 2. Proposal

### Draft Article 4(1) sentence 3 GDPR

It should therefore be clarified, when referring to the relevant CJEU case law, that either draft Article 4(1) sentence 3 GDPR deviates from this case law, or that an adjustment should be made to align with CJEU case law (the “indirect personal reference”). It should be borne in mind, however, that it is questionable whether any amendment to Article 4(1) GDPR is necessary at all if the aim is merely to codify the CJEU case law on the definition of personal data. In that case, even without an amendment to Article 4(1) GDPR, the existing CJEU case law would continue to apply, leaving its further development for new, in particular AI-driven data models. This would offer the advantage of a more flexible solution, as new developments could continue to be taken into account.

### Draft Article 4(1) sentence 1 and 2 GDPR

If the proposal to amend Article 4(1) GDPR is maintained, the following formulation is recommended for draft Article 4(1) sentences 1 and 2 GDPR:

#### *Article 4(1) GDPR*

*“personal data”: all information relating to an identified or identifiable natural person (hereinafter “data subject”); a natural person shall be considered identifiable if they can be uniquely identified, directly or indirectly, by the*

controller or by another person, authority, entity, or body processing such data, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more specific factors reflecting the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Information is not considered personal data for the controller or any other person, authority, entity, or body merely because a third party, who does not process the information, possesses means that could, with sufficient likelihood, be used to identify the natural person to whom the information relates.

Explanation:

This formulation, as part of the “Omnibus” approach, resolves the longstanding problem under Directive 95/46/EC that the definition of “identifiable” appeared circular when the term to be defined was referenced in its own definition: “a natural person shall be considered identifiable if they ... can be identified.”

**f) Amendment of the Rules on Pseudonymisation**

The approach of facilitating compliance with the GDPR by supporting controllers in determining, based on the criteria and means available, whether data resulting from pseudonymisation qualify as personal data or not (Section I, 1.b)), and of incorporating the CJEU’s interpretation of pseudonymisation of personal data into the provisions (Section II, 1.), is to be welcomed.

However, the proposed rules should also be adjusted.

**1. Problem Statement**

Pursuant to Article 4(5) GDPR, “pseudonymisation” means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures

that ensure that the personal data are not assigned to an identified or identifiable natural person.

The CJEU has clarified that pseudonymisation is not an element of the concept of “personal data” itself, but rather concerns the implementation of technical and organizational measures aimed at reducing the risk that a specific dataset can be linked to the identity of the data subject (CJEU, Judgment of 4 September 2025 – C-413/23 P SRB, para. 72). The term “pseudonymisation” presupposes the existence of information enabling the identification of the data subject. The mere existence of such information does not mean that pseudonymised data can in every case be regarded as anonymised data that is excluded from the scope of the GDPR (CJEU, Judgment of 4 September 2025 – C-413/23 P SRB, para. 73).

Pseudonymisation aims to prevent the data subject from being identified solely on the basis of pseudonymised data (CJEU, Judgment of 4 September 2025 – C-413/23 P SRB, para. 74). Where technical and organizational measures are implemented that prevent the attribution of the data in question to the data subject, so that the latter is not or no longer identifiable, pseudonymisation may result in the elimination of the personal reference (CJEU, Judgment of 4 September 2025 – C-413/23 P SRB, para. 75).

When assessing identifiability, all means that are reasonably likely to be used by the controller or another person to directly or indirectly identify the natural person must be taken into account. In determining whether means are reasonably likely to be used for identification, all objective factors should be considered, including the cost of identification and the time required. The technology available at the time of processing and technological developments must also be taken into account (CJEU, Judgment of 4 September 2025 – C-413/23 P SRB, para. 79).

The means employed at the time of processing to protect against re-identification using additional information—particularly the technology used and the effectiveness of measures to remove identifying characteristics—determine whether identification from the pseudonymised data is possible. To the extent that technical and organizational measures ensure that identification is not possible, pseudonymised data constitute

anonymous data for persons who cannot establish a personal reference. Pseudonymisation may therefore have an anonymising effect.

## **2. Proposal for draft Art. 41a GDPR**

The proposed introduction of the new Article 41a GDPR-E addresses pseudonymisation technologies. Under paragraph 1, the EU Commission may adopt implementing acts to establish the means and criteria for determining whether data resulting from pseudonymisation no longer constitute personal data for specific entities. According to the concept outlined by the CJEU, in line with Recital 26 sentence 4 GDPR, these means and criteria determine whether a data subject can be identified from pseudonymised data.

The relationship and significance of this new provision, draft Article 41a GDPR, with respect to the definition of pseudonymisation under Article 4(5) GDPR are not yet clearly regulated in the draft:

- On the one hand, it should be clearly stated that the provisions in draft Article 41a GDPR concern criteria for the technical and organizational measures pursuant to Article 4(5) GDPR. On the other hand, the legal consequences linked to the use of such means remain unclear.
- Draft Article 41a(3) GDPR merely provides that the implementation of the means and criteria established in an implementing act may be used as a criterion to demonstrate that the data cannot lead to re-identification of the data subjects. However, it remains unclear what legal significance this demonstration carries and what its scope should be. It could constitute a rebuttable presumption, in the sense of prima facie evidence, but the wording does not make this mandatory, if the means and criteria are merely used as one criterion among others to demonstrate the exclusion of re-identification. If they are only one criterion among several, it is questionable what practical benefit arises from this demonstration.

A rebuttable presumption would provide controllers with the intended relief in complying with the GDPR as envisaged by the EU Commission. The currently burdensome practical assessment—whether and which recipients of the data possess which means to identify the data subject—would only become relevant if the presumption were rebutted. This would provide legal certainty in the application of pseudonymisation technologies. At the same time, the definition of anonymisation could be added to the GDPR definitions catalogue and clarified—consistent with Recital 26, sixth sentence—that only anonymised data fall outside the scope of the GDPR. Pseudonymised data would then be considered anonymous if identification is unlikely due to the use of the means and criteria established in the implementing act by the EU Commission.

Proposed Article 41a GDPR could read as follows:

#### *Article 41a*

*(1) The Commission may adopt implementing acts to establish the means and criteria for the technical and organizational measures referred to in Article 4(5) GDPR to determine whether data resulting from pseudonymisation no longer constitute personal data for specific entities.*

*(2) For the purposes of paragraph 1, the Commission shall:*

*a) assess the state of available technologies;*

*b) develop criteria and/or categories for controllers and recipients to assess the risk of re-identification in relation to typical data recipients;*

*c) regularly review the available technologies for currency and update the implementing acts in line with technological developments and security requirements.*

*(3) The implementation of the means and criteria established in an implementing act shall give rise to a rebuttable presumption that the data do not lead to re-identification and that the identification of the data subject is excluded.*

*(4) The Commission shall closely involve the European Data Protection Board (EDPB) in the drafting of the implementing acts. The EDPB shall provide an opinion within eight weeks of receiving the draft implementing act.*

*(5) The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93(3).*

In this context, it may be desirable to extract the concept of “anonymisation” from Recital 26 GDPR and include it in the definitions catalogue of Article 4 GDPR. The definition set out in Recital 26 should be amended, taking into account the complements regarding pseudonymisation, to clarify which data are considered pseudonymised and which are anonymised:

*Article 4(5a) GDPR*

“Anonymisation” means the processing of personal data in such a manner that such data no longer relate to an identified or identifiable natural person, and the data subject cannot be identified, either directly or indirectly. In determining whether a natural person is identifiable, all means that are reasonably likely to be used by the controller or by another person processing the data to identify the natural person, directly or indirectly, shall be taken into account.

Pseudonymised data (within the meaning of Article 4(5) GDPR) shall be considered anonymised if it is excluded that the means available to the controller or to another person processing such data could directly or indirectly enable the identification of the natural person.

**g) Other proposed amendments, in particular to the Data Act**

The DAV generally welcomes the European Commission’s efforts to simplify the Data Act (Regulation (EU) 2023/2854) within the framework of Proposal COM (2025) 837 final and to expand it into a comprehensive data code. The Commission’s proposal contains approaches to strengthening the rights of data holders, improving the protection of trade secrets, and facilitating international data transfers, which, however, do not yet adequately capture the practical problems in these areas. Detailed analysis still reveals significant deficits in these essential fields; the DAV respectfully requests that it be carefully examined whether, in these regulatory areas, the following proposals can create greater legal certainty and a better balance of interests among the stakeholders involved. This also fundamentally concerns the relationship between the Data Act and the GDPR.

The DAV subsequently points out specific areas requiring improvement and submits precise proposals for the optimization of the regulatory proposal.

## **1. Relationship of an Expanded Data Code to Data Protection provisions**

A consolidation of data law provisions in a single regulation facilitates clarity regarding the relevant rules and is to be welcomed. However, the actual challenges in legal application are not resolved if (1) the relationship to data protection regulations, in particular the GDPR, remains unregulated, and (2) existing provisions that do not achieve the intended effects in practice—such as the Data Governance Act—are adopted without sufficient revision.

Pursuant to Article 1(5), the Data Act applies “without prejudice” to, *inter alia*, the GDPR. Consequently, the relationship between the Data Act, the GDPR, and the other legal instruments listed in Article 1(5) for the protection of personal data, privacy, the confidentiality of communications, and the integrity of end devices relevant to personal data, is highly complex in application. In particular, the assessment risk—whether a data protection legal basis exists for access to data under the Data Act or, in the future, for the processing of personal data by data intermediary services or data altruistic organisations—is largely shifted to the level of the legal users. These users, for example under Chapter II of the Data Act, are obliged to grant access to data; if a data protection legal basis exists, access must be granted, whereas if such a basis does not exist, access must not be granted. Whether a data protection legal basis exists is often the subject of a complex assessment and a case-by-case balancing of interests, which only occasionally yields clear results.

As also envisaged, for example, in Regulation (EU) 2025/327 on the EU Health Data Space, the assessment risk should, in view of this, be shifted to the competent authorities. At a minimum, actors obliged to grant data access should be granted a right to refer the matter to an authority in order to obtain—a procedure comparable to the data approval under the EU Health Data Space regulation—a binding decision by the authority on the obligation to grant access or, if no data protection legal basis exists, on the obligation not to do so.

The current proposal COM (2025) 837 final, however, does not foresee any amendments to Article 1(5) Data Act. The DAV suggests that this should be reconsidered in the sense outlined above.

## **2. Proposed Amendments to the Definitions in Article 2 Data Act**

### **a) Definition of “Data Holder”**

The new definition—particularly the insertion of the comma in the last clause—is neither sufficiently clear nor does it resolve the practical issues associated with the definition. We interpret the comma as clarifying that the subordinate clause is not determinative and therefore does not relate to “product data.” This makes it clear, for the variant of connected service data, that the data holder must effectively be in a position to make the data accessible, and that only a person in such a position can be considered a data holder. For product data, no comparable statement exists. However, in German legal literature and ultimately in the Commission’s FAQs, it is assumed that this requirement applies (see Commission FAQ on the Data Act, Version 1.4, Question 34). This should also be clarified. For example, a manufacturer that offers a digital product which generates product data, without a connected service or other access mechanism, is generally not in a position to make data accessible under Article 4 Data Act. Such a manufacturer may only fall under Article 3 Data Act.

According to prevailing opinion in German legal literature, the definition of “data holder” is circular (sometimes described as “confusing” or “unusable”). This arises, inter alia, because the obligation to make data accessible primarily derives from Article 4 Data Act if no other provisions apply, whereas Article 4 Data Act, in turn, addresses the data holder. The DAV recommends urgently eliminating this circular element, unless it is intended to imply that a contractual (or other statutory) entitlement is required, as occasionally suggested in the literature. In that case, the definition should alternatively be phrased more clearly.

Further difficulties arise because there may be situations in which, based on the Commission’s principle that a user cannot be a data holder (see Commission FAQ on

the Data Act, Version 1.4, Question 34), no data holder exists, but there is one user with data access and another without. The second user would then have no entitlement to data access. This is particularly relevant in situations such as rental or leasing within the contractual chain. If one intends to open data silos, it should be clarified either that the first user simultaneously is also a data holder—requiring adjustments to, inter alia, Articles 4(12) and 4(13) Data Act so as not to prohibit users from handling their own data—or that the rights under Articles 4 and 5 must also be enforceable against users where no data holder exists.

It should also be noted that German legal literature occasionally advocates a relative concept of the data holder. This approach could also resolve the problem, but would require clarification. With regard to Recital 22 Data Act (“Processors within the meaning of Article 4(8) of Regulation (EU) 2016/679 shall not be regarded as data holders”), it is additionally unclear in which situations a processing arrangement excludes the contractor’s data holder status, in particular whether the rule set out in Recital 22 applies only to processing pursuant to Article 28 GDPR, i.e., in relation to personal data. A differentiated treatment depending on the personal reference of the data would be difficult to justify and, in practice, very hard if not impossible to implement.

#### **b) Concept of Re-use**

We suggest that the definition of “re-use,” as it is to be introduced in Article 2(52) of the new Data Act, should be more clearly delimited. The term “re-use” is defined there for the provisions that are to be transferred from the Data Governance Act into the Data Act. For this specific context, the definition is appropriate. However, if “re-use” is defined in such a restrictive manner for the Data Act as a whole, as currently proposed, this would not reflect general practice. For instance, data obtained through data access mechanisms are also “re-used,” even though such data do not constitute documents held by public sector bodies or public undertakings, as provided for in the legal definition of the new Article 2(52) Data Act.

The definition should therefore be specifically limited to provisions concerning the use of data held by public sector bodies, for example by being worded as follows:

*“52. ‘re-use under Chapter VIIc’ means the use ...”*

Accordingly, the definition in Article 2(57) should also be amended:

*“57. ‘re-user under Chapter VIIc’ means a natural or legal person ...”*

Furthermore, the terms should not be restricted to the re-use of documents, since Article 32i of the proposed Regulation—correctly—also covers the re-use of data.

### **3. Obligations of Manufacturers Regarding Data Accessibility by Design and Their Relationship with the Data Holder**

Article 3(1) of the Data Act obliges manufacturers to design and manufacture connected products, and to design and provide related services, in such a way that the relevant product data and related service data are “directly accessible.” This product design obligation—namely, to enable data access through the design of the product itself—constitutes a key cornerstone of the data access regime set out in Chapter II of the Data Act. However, there is a lack of clear regulation regarding the legal consequences, enforceability, and interaction with the obligations of the data holder to make the data available, potentially including making such data available to a data recipient even in cases where data accessibility by design has been implemented. This should be clarified in the course of the legislative revision.

In addition, it remains unclear what is meant by the term “direct access” and how the relationship between the data holder and the manufacturer is to be understood. In this respect, reference is made to the DAV Position Paper No. 40/2022, which remains relevant on these points.

Furthermore, in relation to the current version of Article 3(1) of the Data Act, the Commission appears to assume that the manufacturer enjoys a certain degree of discretion as to whether or not to make the data accessible. It bases this view on the wording “where relevant and technically feasible” (see the Commission’s FAQ on the Data Act, version 1.4, question no. 22). However, it overlooks the fact that the same

wording in Article 4(1) of the Data Act is clearly intended to establish a binding obligation. Moreover, both the legislative history and the objective of the Data Act—namely, to facilitate data access—militate against such an interpretation. The question of discretion should therefore be clarified by the legislator and, if necessary, revised accordingly.

#### **4. Developments Concerning the Protection of Trade Secrets, in Particular under proposed Articles 4(8) and 5(11) of the Data Act**

Should such clarification not be undertaken, manufacturers should be granted rights (defences) similar to those provided for under Articles 4(8) and 5(11) of the Data Act proposal. Alternatively, in cases requiring the protection of trade secrets, manufacturers should be afforded the possibility to safeguard themselves against data access requests and to grant such access only under the conditions set out in Articles 4(8) and 5(11) of the Data Act proposal.

The clarifying addition (“it is highly likely ... or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law”) is to be welcomed. Indeed, there is a significant risk that trade secrets and know-how of European undertakings may be unintentionally disclosed and incorporated into competing products. In this context, it should even be considered whether the right to refuse access ought to be explicitly extended to cases in which the data, as derived information, would facilitate the inference—by way of reverse engineering—of particularly valuable technical know-how. One possible addition could read as follows:

*“It is highly likely ..., or where, by virtue of the data to be made accessible, core know-how underlying a product or service—beyond such data—is indirectly disclosed or can be more readily obtained through reverse engineering.”*

## 5. Provisions on Data Use in Contracts

Article 13 of the Data Act regulates unfair contractual terms concerning data access and data use in business-to-business relationships. Ensuring fair contractual terms is a legitimate and welcome objective. However, the DAV suggests that the provisions should be revised in detail, as they currently lead, in certain respects, to excessive and unjustified restrictions.

We propose that the following amendments be introduced in Article 13 of the Data Act:

The terms used in Article 13(4) and (5) should be clarified by means of clear legal definitions and applied consistently:

- “Non-performance” should cover all cases of failure to perform the contractually owed obligation.
- “Breach of contractual obligations” should refer to defective or non-compliant performance.
- “Liability” should refer to claims for damages.
- “Remedies” should encompass all contractual and statutory remedies, including termination, price reduction, and damages.

The exclusion of liability for the slightly negligent breach of contractual obligations should, in principle, be permissible in a comprehensive manner. This is not clearly reflected, in particular, in Article 13(4)(b) and (5)(a) of the Data Act. In these provisions as well, liability should be limited to intentional or grossly negligent conduct, as is already the case in Article 13(4)(a) of the Data Act.

It should also be clarified in the recitals that, in the context of online contracts concluded via an “accept” button, the requirement of negotiation is deemed to be fulfilled where the user was explicitly informed, prior to the conclusion of the contract, of the possibility to make contact for the purpose of negotiations.

## **6. Amendments to Chapter V – Provision of Data to Public Sector Bodies**

The proposed Regulation envisages a significant restriction of the rules on the obligation to make data available to public sector bodies by deleting Articles 14 and 15 of the Data Act in Chapter V and introducing a new Article 15a, which limits such data sharing obligations to situations of public emergency. This approach is welcomed by the DAV.

## **7. Amendments in Chapter VI on Switching Data Processing Services**

The DAV also welcomes the proposed amendments to Chapter VI, in particular the exemptions from the scope for services tailored to specific customer needs and the authority to impose sanctions in cases of early termination. However, the adjustments should go further to better safeguard the appropriateness and proportionality of the intervention in private autonomy associated with these rules.

The threshold at which services tailored to customer needs are exempted from the scope must be clearly defined. At present, this is attempted through the formulation “the majority features and functionalities.” In practice, this is likely to lead to significant delineation problems and circumvention risks, as a purely quantitative assessment could be used to evaluate numerous insignificant functions, whereas the qualitative assessment—whether the product is standardized or genuinely individualized—should be decisive. This could, for example, be based on the proportion of remuneration attributable to customizations and individualizations, which must be broken down according to objective criteria.

The authority under Article 31(1b) of the proposed Regulation to impose proportionate sanctions for early termination corresponds to market needs for more flexible contract durations than currently allowed. Customers also frequently require the ability to enter into longer-term contracts than the current framework provides (30 days plus 2 months for termination during a switch). However, the current provision is insufficient to achieve a balanced relationship between contractual freedom and market access. It should be explicitly permitted to offer different options with varying contract lengths, provided that

the conditions across the options are reasonable and non-discriminatory. Business customers can be reasonably expected to choose in advance between genuine and fair alternatives. If a customer selects a longer-term contract, they must be bound by that choice.

It also remains unclear what contractual consequences arise if the provider violates the obligations under Article 25 of the Data Act. Are the provisions required by the Data Act but not included in the contract incorporated into the contract via supplementary interpretation? Does the customer have a right to the inclusion of supplementary contractual clauses? Or does a breach of Article 25 Data Act have no contractual effect? Clarification on this point is also needed.

## **8. Clearer Rules for Securing International Data Transfers**

The proposed amendments in the area of international data transfers provide simplification and clarification. However, the wording of Article 32(1) should be more closely aligned with Article 32 GDPR to avoid ambiguities in interpretation and application:

*“... shall take all adequate technical, organizational and legal measures, considering the state of the art, implementation costs, and the likelihood and severity of risks, to ensure a level of protection appropriate to the risk, in order to prevent governmental access to non-personal data stored in the Union or transferred to third countries by entities from third countries, where such access would conflict with Union law or the national law of an EU Member State, without prejudice to paragraph 2 or 3.”*

The DAV further suggests that the EU Commission should, for the recognition of equivalence of international treaties or equivalent arrangements, adopt implementing acts comparable to adequacy decisions under Article 45 GDPR, thereby facilitating the assessment for individual entities.

## **9. Consolidation of Data Law Provisions in the Data Act**

The DAV expressly welcomes the consolidation of data law provisions in the Data Act. However, the revision of the Data Governance Act provisions does not go far enough to strengthen its practical relevance or achieve the objective of increasing the provision of data intermediary services and the registration of data altruistic organizations. The deletion of provisions on the European consent form should be reversed and such a form developed, as it could significantly enhance legal certainty for data altruistic organizations, which often have limited resources for legal advice and other risk mitigation measures.

## Mailing List

---

### Europe

#### European Commission

- Directorate-General for Communications Networks, Content and Technology (DG CNECT)
- Directorate-General for Justice and Consumers (DG JUST)

#### European Parliament

- Committee on Legal Affairs (JURI)
- Committee on the Internal Market and Consumer Protection (IMCO)
- Committee on Civil Liberties, Justice and Home Affairs (LIBE)

#### Council of the European Union

Permanent Representation of the Federal Republic of Germany to the European Union

Legal Advisors of the Permanent Representations of the Länder to the European Union

Council of Bars and Law Societies of Europe (CCBE)

Bundesverband der Freien Berufe (BFB) – Brussels Office

Deutsche Industrie- und Handelskammer (DIHK) – Brussels Office

Bundesverband der deutschen Industrie e.V. (BDI) – Brussels Office

### Germany

Bundesministerium des Innern

Bundesministerium der Justiz und für Verbraucherschutz

Bundesministerium für Wirtschaft und Energie

Bundesministerium für Digitales und Staatsmodernisierung

Ausschuss für Inneres im Deutschen Bundestag

Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag

Ausschuss für Wirtschaft und Energie im Deutschen Bundestag

Ausschuss Digitale Agenda im Deutschen Bundestag

Fraktionen im Deutschen Bundestag

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Justizministerien der Länder

Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland

Bundesrechtsanwaltskammer

Bundesnotarkammer

Bundesverband der Freien Berufe e.V.

Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und

Bund Deutscher Verwaltungsrichter und Verwaltungsrichterrinnen

Staatsanwälte e.V. (DRB)

Deutscher Notarverein

Deutscher Steuerberaterverband e.V. Berlin

Bundesverband der Deutschen Industrie e.V.

Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.

Deutscher EDV-Gerichtstag e.V.

GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.  
Bitkom e. V.

Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)

ver.di - Vereinte Dienstleistungsgewerkschaft

Gewerkschaft der Polizei

Deutsche Polizeigewerkschaft im DBB (DPoIG)

DAV-Vorstand und Geschäftsführung

Vorsitzende der DAV-Gesetzgebungsausschüsse

Vorsitzende der DAV-Landesverbände

Vorsitzende des FORUMs Junge Anwaltschaft

### Press

Frankfurter Allgemeine Zeitung GmbH

Süddeutsche Zeitung GmbH

Redaktion NJW

JUVE Verlag für juristische Information GmbH

Redaktion Legal Tribune Online / LTO

Redaktion Anwaltsblatt

juris GmbH

Redaktion MultiMedia und Recht (MMR)

Redaktion Zeitschrift für Datenschutz ZD

Redaktion heise online

DER SPIEGEL GmbH & Co. KG

Computer und Recht