

Making Simplification and Improvement Come True – ELI’s Proposed Revisions to the Digital Omnibus

European Law Institute





Feedback of the European Law Institute on the
Digital Omnibus – COM(2025) 836 and 837 final

Making Simplification and Improvement Come True – ELI's Proposed Revisions to the Digital Omnibus

The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment, it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

President: Teresa Rodríguez de las Heras Ballell
First Vice-President: Sir Geoffrey Vos
Second Vice-President: Pietro Sirena
Treasurer: Anne Birgitte Gammeljord
Speaker of the Senate: Reinhard Zimmermann
Secretary-General: Vanessa Wilcox
Scientific Director: Christiane Wendehorst

European Law Institute
Schottenring 16/ 175
1010 Vienna
Austria

Tel: + 43 1 4277 22101
Email: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

Approved by the ELI Council on 11.03.2026.

Published on 11.03.2026.

ISBN: 978-3-9505990-2-2
© European Law Institute 2026

Acknowledgement is due to the University of Vienna, which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011.



Acknowledgements

Authors

Christiane Wendehorst (Professor of civil law and deputy head of the Department for Innovation and Digitalisation in Law at the University of Vienna, Austria)

Paolo Balboni (Professor of privacy, cybersecurity, and IT contract law at the European Centre on Privacy and Cybersecurity (ECPC) of Maastricht University, the Netherlands, and partner at ICT Legal Consulting)

Moritz Hennemann (Professor of private law, information, media, and internet law, co-director of the Institute of Media and Information Law at the University of Freiburg, Germany, and judge at the Higher Regional Court (OLG) Karlsruhe)

Jussi Mäkinen (Legal and policy expert specialising in EU data and digital regulation, Technology Industries of Finland, Helsinki, Finland)

Bernhard Nessler (Research Manager Intelligent Systems and Certification of AI at the Software Competence Center Hagenberg, lecturer at the Institute for Machine Learning at the Johannes Kepler University Linz and Vice-President of the Austrian Society for Artificial Intelligence (ASAI), Austria)

Teresa Rodríguez de las Heras Ballell (Professor of commercial law at Universidad Carlos III de Madrid and a delegate of Spain to UNCITRAL and UNIDROIT on digital economy projects)

Agata Szeliga (Attorney at law, partner at Sołtysiński Kawecki & Szlęzak in charge of the personal data and privacy law practice, Warsaw, Poland)

Rania Wazir (Data scientist and mathematician working on human rights-based AI technology, co-founder and CTO of leiwand.ai, delegate to international standards organisations working on AI)

Project Assistants

Gregor Aichinger (Data Protection Officer at Voestalpine Group-IT and Lecturer at the Johannes Kepler University Linz)

Raphael Ezeudji (Research Assistant, University of Vienna)

ELI Project Officers

Tomasz Dudek (Senior Project Officer, European Law Institute)

Marta Lages de Almeida (Project Officer, European Law Institute)

Table of Contents

Executive Summary	8
I. Introduction	10
1. Simplification of the digital acquis is overdue – but let’s get it right	10
2. More risk-based data protection – relationship to ELI’s 2025 response	10
3. True simplification requires a fully redrafted ‘Data (Economy) Act’	11
4. Digital legislation needs a comprehensive ‘European sovereignty check’	11
II. Amendments to the AI Act	12
1. A split Digital Omnibus on AI with fixed dates of application	12
Splitting Proposal COM(2025) 836 to ensure timely adoption	12
Introducing fixed dates instead of dependency on a Commission Decision	13
2. Moving a simplified rule on special categories of data to Article 9 GDPR	13
III. Amendments to the GDPR	15
1. Codifying the CJEU’s judgment in <i>EDPS v SRB (C-413/23 P)</i>	15
2. Creating legal certainty for AI development and operation	17
A more technology-neutral solution that addresses the most salient points	17
Legal certainty regarding AI output and its relationship with the AI system or model	21
3. Removing general uncertainties around special categories of personal data	23
Restricting Article 9 to sensitive processing operations	23
Additional grounds for the permitted processing of special categories of personal data	24
IV. Consolidation of four legal instruments into a Data Act 2.0	26
1. Most urgent revisions in Chapter I	26
Scope of the Data Act	26
Definition of ‘data holder’	29
Simplification and revision of other definitions	30
2. Most urgent revisions in Chapters II and III (mandatory data sharing)	31
Clarifying the data holder’s right to refuse sharing data for trade secrets protection	31
Replacing Article 4(13) and (14) by a separate provision on the data holder’s use of data	32
Eliminating errors and ambiguities by re-drafting Articles 7, 8, 11 and 12	33
3. Most urgent revisions in Chapter VI (cloud switching)	37
A simpler regulatory technique and more legal certainty concerning customer rights	37
A more transparent provision on charges	39
4. Most urgent revisions in Chapter XI	41
ANNEX: Visualising proposed amendments to the Digital Omnibus	43
1. Redrafting that aims at substantive changes	43
AI Act	43
GDPR	46
Data Act	51
2. Editorial redrafting that eliminates errors, inconsistencies and ambiguities	54

Executive Summary

ELI's response endorses the Commission's simplification agenda, including the proposal for a 'Digital Omnibus' in COM(2025) 836 and 837 final, as a timely step to reduce regulatory fragmentation and strengthen legal certainty. While broadly supportive of the overall direction, ELI puts forward a targeted set of proposed amendments. Given the short timeframe for this consultation and the limited scope for changes, it has focused on a small number of key points.

1. Concerning the **Artificial Intelligence Act (AI Act)**, the proposal to condition the application of core highrisk requirements on future Commission decisions would create a complex and uncertain calendar, discouraging early compliance or compressing timelines once decisions are passed. To restore certainty and market confidence, the package should be split so that an amended Article 113 AI Act is adopted immediately with clear, fixed dates, replacing conditional triggers with a single, definite application date for pending provisions.

2. With regard to the targeted reform of the **General Data Protection Regulation (GDPR)**, ELI builds on its 2025 call for a more riskbased approach to EU data protection law, but restricts itself, in this 2026 response, to some few particularly important aspects that seem to fit within the scope envisioned by the Commission for the Digital Omnibus.

ELI supports the Commission's proposal to codify *EDPS v SRB* (C-413/23 P) in Article 4(1) GDPR. However, ELI would like to draw attention to certain discrepancies between the CJEU's judgment and what is proposed in COM(2025) 837 and recommend a slightly different approach. Certain safeguards must prevent loopholes in downstream transfers of pseudonymised data and ensure adequate data security where it cannot be ruled out that recipients have means to identify the data subjects. Also, the mere legal prohibition of re-identification 'on paper' cannot suffice for making data anonymous for a party.

To support AI development while safeguarding fundamental rights, ELI recommends adopting a more technology neutral version of the proposed

Article 88c GDPR that is not limited to the narrow definition of an 'AI system' under the AI Act. ELI further recommends that this provision address the practical difficulties in establishing a legal basis under Articles 6 and, where relevant, 9 GDPR for each individual data point, as well as the challenges of immediate compliance with certain obligations and data subject rights where such compliance would entail disproportionate effort. ELI also proposes introducing a new Article 88d GDPR to clarify when AI outputs constitute personal data, who is the controller, and what is the relationship to the system or model itself.

Bias detection and correction should be facilitated by introducing a dedicated legal basis into Article 9(2) GDPR, rather than relying on the AI Act's narrow and complex Article 10(5) or the now-proposed new Article 4a AI Act, as the broader GDPR basis would support antidiscrimination efforts across technologies and ensure uniformity in competent authorities. Complementing this, Article 9(2) GDPR should also include a contractbased ground to reduce unnecessary reliance on explicit consent in day-to-day activities. More generally, the uncertainties around special categories should be addressed by refocusing Article 9(1) GDPR on sensitive processing operations to avoid the paralysation of the European digital economy that could potentially follow from recent CJEU case law in the area.

3. ELI also supports the Commission's proposal to **consolidate the data-related acquis by merging the Data Act, Data Governance Act, Free Flow of Data Regulation, and Open Data Directive**. However, at least in the medium term, ELI pleads for a freshly drafted, integrated 'Data Economy Act' rather than transplanting provisions into the current Data Act in a way that risks creating an even more complex patchwork.

Within the Data Act, both in its existing form and considering the proposed amendments, urgent clarifications and simplifications are recommended. The approach currently taken in some provisions of the Data Act to have mutually exclusive regimes for personal and for non-personal data seems to be hardly manageable for businesses, and the situation may

become worse after *EDPB v SRB*. Rather, there should be one baseline regime for all data under the Data Act, with the GDPR applying in addition to that regime where data is personal data. ELI also recommends avoiding any retroactive effect of Chapters II and VI of the Data Act that results in massive challenges for European businesses and potentially puts them at a significant competitive disadvantage, considering also shortcomings in the territorial scope.

With these two exceptions, ELI's proposals on the Data Act are limited to editorial redrafting, including the correction of evident legislative errors and removal of ambiguities, and do not seek to alter policy choices. That said, where provisions are so unclear that their meaning cannot be discerned, even clarification may inevitably entail some substantive decisions. In cases where substantive decisions would have been too obvious and far-reaching – such as reworking the manifestly unclear definition of 'data processing service' – ELI has refrained from proposing a concrete alternative draft.

In Chapter I, Article 1 should be revised. It is unnecessarily complex, risks misinterpretation, and – likely due to drafting errors – defines the territorial scope in a way that massively disadvantages European businesses compared with those in third countries. Within the list of definitions in Article 2, that of 'data holder' must be replaced, as it is both circular and clearly inconsistent with the EU legislator's intent.

As concerns Chapters II and III on data sharing, the data holder's right to refuse sharing for trade secret protection should be phrased in a more transparent manner, and a new Article 3a should govern the data holder's own use of product and related services data, replacing the current convoluted provisions in Article 4(13) and (14). It is also recommended to correct several errors, inconsistencies and ambiguities in Articles 7, 8, 11, and 12, such as avoiding that obligations designed for businesses rest on consumers, ensuring a degree of party autonomy consistent with Recital 25, separating technical safeguards from remedies, and correctly defining the scope of Chapter III.

For Chapter VI on cloud switching, the regulatory approach should be simplified and provide for clear and strong customer rights. Article 25 should be split into a contract-focused Article 25 and a new Article 25a that clearly sets out a list of statutory and directly enforceable switching rights together with a transparent description of the relevant timelines and modalities. ELI also proposes a clearer and more transparent provision on charges in the context of switching in line with Recital 89 and provides essential guidance on the conditions under which early-termination penalties are consistent with the prohibition of switching charges.

I. Introduction

ELI is pleased to submit its feedback to the European Commission's ex post consultation on the Digital Omnibus proposals, COM(2025) 836 and 837 final, published on 19 November 2025. We welcome this opportunity to engage with the Commission and the EU legislator and to share our practical and comparative legal expertise. Our submission seeks to support the consultation's objectives by offering constructive observations and targeted recommendations to enhance legal clarity, provide better protection for the rights of citizens and businesses, and enhance economic competitiveness and growth in Europe.

1. Simplification of the digital acquis is overdue – but let's get it right

Over the past decade, the EU has created a robust framework for the digital economy. With a growing number of legislative instruments businesses must comply with, there is a growing need for simplification and better alignment to avoid regulatory fragmentation and unnecessary complexity, and to ensure that laws are consistent and provide the degree of legal certainty which businesses need in order to flourish. The Commission's recent simplification initiative, including the Digital Omnibus Proposal, comes just in time and is an important step towards better competitiveness and growth.

ELI fully endorses the Commission's new simplification agenda, encouraging the Commission to move forward both with the Digital Omnibus Proposal and further omnibus proposals still to come. However, given that too frequent revisions would cause disruption for businesses in Europe, ELI urges the European legislator to re-consider several points in the current Proposal.

For this reason, ELI, in this response to the ex-post consultation, submits a number of proposals as to how COM(2025) 836 and 837 could be improved during the legislative process. Given the short timeframe for this consultation and the limited scope for changes, it has, so far, focused on a limited number of key points.

2. More risk-based data protection – relationship to ELI's 2025 response

On 14 October 2025, ELI published a response to the Commission's public consultation on the Digital Omnibus ('**Simpler, Fairer, More Effective – Towards a Targeted Revision of EU Data Protection Law**'). It focused on urging the Commission to include a targeted revision of the General Data Protection Regulation (GDPR) in the Digital Omnibus, which had so far not been mentioned in the consultation documents. ELI is pleased to note that the Commission has, indeed, decided to propose targeted revisions to the GDPR, whose general aim is very much in line with ELI's proposals.

In this 2026 ex-post response, ELI reiterates only some of the proposals from 2025 and largely confines itself to the issues already addressed in the Digital Omnibus Proposal. However, ELI upholds the entirety of the amendments it proposed in its response of 14 October 2025 and urges the Commission to consider them as part of the broader Data Union Strategy.

In essence, ELI proposed a risk-based approach that takes regulatory burdens off SMEs and facilitates the development and deployment of AI and other technologies, while also offering significant data protection enhancements in scenarios where citizens' fundamental rights are manifestly at risk. Among others, ELI proposed:

- to define a black-list of 'prohibited data processing' operations that are so harmful that they cannot be justified even by the consent of the data subject, as well as a white-list of 'exempted data processing' operations that are no longer subject to the GDPR.
- to introduce a three-layered regulatory regime within the GDPR: an 'enhanced regime' for big, sophisticated players in the digital economy engaging in high-risk data processing; a 'light regime' for small, non-sophisticated players processing personal data in their day-to-

day activities without engaging in high-risk processing; and a 'regular regime' for all other cases.

3. True simplification requires a fully redrafted 'Data (Economy) Act'

Beyond data protection, there is an urgent need to harmonise the various legal instruments that focus on the data economy, often with a particular focus on non-personal data. ELI therefore fully endorses the Commission's proposal to merge four legal instruments in the field of data law, namely the Data Act (DA, Regulation 2023/2854), the Data Governance Act (DGA, Regulation 2022/868), the Free Flow of Data Regulation (FFDR, Regulation 2018/1807) and the Open Data Directive (ODD, Directive 2019/1024). However, ELI wishes to point out that it may not be appropriate to transfer all surviving provisions into the existing DA, given that this results in a patchwork that may be even more difficult for businesses to understand and comply with than the original legal instruments. Also, it must be borne in mind that the DA is held to be a particularly problematic piece of legislation, suffering from an astonishing number of unintelligible provisions, drafting errors, redundancies and inconsistencies (see, eg, below at IV.2) after a rushed legislative procedure without proper scrutiny.

While, in this response, ELI confines itself to some few 'crunch points' that create massive problems from a substantive point of view, ELI wishes to emphasise that true simplification of the data-related acquis would require merging the DA, DGA, FFDR and ODD in a fully redrafted new legal instrument.

This new legal instrument could be a 'Data Economy Act', or an entirely new 'Data Act' that replaces the current one.

4. Digital legislation needs a comprehensive 'European sovereignty check'

ELI also wishes to underline the urgent need to assess both existing and forthcoming EU legislation through the lens of Europe's global competitiveness and strategic autonomy, particularly in light of recent geopolitical shifts and growing concerns about digital sovereignty in technologies and the digital economy. In this submission, ELI identifies several provisions that – most likely unintentionally – create significant disadvantages for European businesses compared with competitors established in third countries.

By way of example, Union-based holders, eg, of data from connected vehicles, have had to cease using such data – for instance, for AI development or other innovation – from 12 September 2025 unless they were able to agree new terms with the vehicle users. By contrast, third-country data holders of comparable data might fall outside the Data Act's scope unless to the extent that they 'make data available to data recipients in the Union' (cf. Article 1(3)(c) – most likely one of the many drafting errors in the Data Act), and this asymmetry is still compounded by practical enforcement challenges vis-à-vis operators located outside the EU. More generally, the Data Act imposes extensive data-sharing obligations on sectors in which Europe has traditionally been strong (such as automotive, aerospace, and machinery), effectively requiring EU-based data holders to make valuable industrial data, including trade secrets, available at marginal or no remuneration to more or less any user or party designated by a user.

ELI urges the Commission and EU legislator to subject all existing and new legislation on the digital economy to a 'European sovereignty check', ensuring that EU legislation is in line with European strategic interests.

II. Amendments to the AI Act

1. A split Digital Omnibus on AI with fixed dates of application

Pursuant to Article 113 of the AI Act, the Regulation's entry into application will occur in stages. Under the current provision, the rules for high-risk AI systems will apply as of 2 August 2026 – the general date of application under Article 113(2) – or 2 August 2027, pursuant to point (c) in Article 113(3).

In response to implementation challenges, such as delays in adopting harmonised standards, common specifications, and the Commission's expected guidelines, the Commission proposes, in the Digital Omnibus Proposal, to postpone the application of certain provisions. To that end, the Commission proposes adding new points (d) and (e) to Article 113(3) of the AI Act, making the application of Chapter III, Sections 1, 2, and 3 (the core requirements for high-risk AI systems) conditional upon the adoption of a Commission decision confirming that adequate measures supporting compliance with Chapter III are available. Application would then occur within a set period (6 or 12 months) after the adoption of such a decision or, in the absence of such a decision (or if these dates are earlier) on 2 December 2027 for AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and on 2 August 2028 for Chapter III, Sections 1, 2, and 3.

ELI considers the postponement regrettable, particularly in relation to the main provisions governing high-risk AI systems, which are the core of the AI Act. Nevertheless, if the postponement is deemed inevitable due to delays in providing adequate measures to support compliance, ELI urges the Commission to consider a substantial change to the drafting of Article 113 in the Digital Omnibus Proposal.

Splitting Proposal COM(2025) 836 final to ensure timely adoption

ELI considers that the proposed Article 113 in the Digital Omnibus Proposal increases uncertainty

for compliance actions and strategies and imposes additional burdens on operators in planning their compliance. Operators may be discouraged from beginning implementation until the Commission adopts the expected decisions, and a 6- or 12-month window may be too short to complete compliance plans. Alternatively, if operators postpone compliance until the decision is approved and the decision is delayed to the point that the back-up dates become the deadlines, operators could be forced into compliance without the expected guidance. In fact, if the lack of adequate compliance-support measures is deemed sufficiently decisive to justify a postponement, then, in the absence of a Commission decision confirming that such measures are available, it would not be reasonable for Chapter III to apply nonetheless (on 2 December 2027 or 2 August 2028).

Furthermore, the publication of the Digital Omnibus Proposal has created a disconcerting situation and heightened uncertainty. Operators must wait for the adoption of the Digital Omnibus to know whether 2 August 2026 and 2027 remain relevant and, if not, how the revised Article 113 will finally be drafted. Such an impasse is highly inadvisable and detrimental to market efficiency and trust. ELI therefore considers that the decision on the new application calendar must be adopted immediately to reduce uncertainty and must be clarified and simplified.

ELI urges the Commission to divide the Digital Omnibus on AI into two parts. The proposal concerning Article 113 of the AI Act should be adopted immediately in order to provide operators with clarity and certainty about the application dates.

Decisions on the proposals relating to other provisions of the AI Act may take longer and require further deliberation. Any delay in deciding the date of application would be highly inconvenient and regrettable.

Introducing fixed dates instead of dependency on a Commission Decision

The proposed additions in the Digital Omnibus Proposal not only make Article 113 of the AI Act a complex provision, but they also create a complicated and conditional application timeline.

A clear and certain application date is crucial for operators potentially subject to the AI Act. Certainty and predictability in the application of the Regulation's provisions will enable operators to plan compliance actions, deploy strategies in a timely manner to adapt their business models and commercial practices to the AI Act, and make reasoned decisions when providing, placing on the market or putting into service, and using AI systems and AI models. Making the date of application conditional upon a Commission decision – even with an additional 6- or 12-month period before the provisions take effect, does not provide reasonable certainty about the AI Act's application. Moreover, it makes the Regulation's application dependent on a Commission action, which could be seen as problematic.

ELI takes the view that the date of application should not be made conditional upon the adoption of a decision by the Commission: rather, it should be set by clear and fixed dates.

ELI therefore recommends determining fixed, clear application dates for the pending provisions of the AI Act, for example by simply deleting the part on the Commission decision, which could mean the following drafting of Article 113:

Article 113

Entry into force and application

1. **This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.**
2. **It shall apply from 2 August 2026.**
3. **However:**
 - a. **Chapters I and II shall apply from 2 February 2025;**

- b. **Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101;**
- c. **Chapter III, Sections 1, 2, and 3, shall apply**
 - i. **on 2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and**
 - ii. **on 2 August 2028 as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I;**
- d. **Articles 102 to 110 shall apply from [the date of entry into application of the Digital Omnibus Regulation].**

2. Moving a simplified rule on special categories of data to Article 9 GDPR

The AI Act includes a very complicated provision on the processing of special categories of personal data in its Article 10(5). This is very unfortunate, not least because the scope of Article 10(5) AI Act is restricted to high-risk AI systems, while the need to avoid bias and discrimination is a general need that also concerns other AI systems and general-purpose AI models. In the Digital Omnibus Proposal, the Commission now proposes moving the provision to Chapter I of the AI Act.

While ELI endorses the decision to allow for bias detection and correction and the avoidance of discrimination on a broader scale, it still believes that the proposed solution is sub-optimal in several respects:

- There is no reason for having this provision within the AI Act instead of in the GDPR once a decision has been made to make targeted amendments also to the latter. The provision should therefore be transferred to the GDPR.

- Transferring the provision to the GDPR would move the matter from the competence of market surveillance authorities to that of data protection authorities, which is more appropriate and would help avoid governance frictions and divergent decisions by national authorities.
- The scope of application still depends on whether a system qualifies as an AI system. However, the definition of an AI system in Article 3(1) AI Act is highly unclear and potentially very narrow, and the need for bias detection and correction and the avoidance of discrimination also applies to other technology.
- The manner in which the proposed Article 4a AI Act is phrased sounds extremely daunting, seemingly discouraging bias detection and correction by treating them in a much stricter way than any of the other grounds for processing special categories of personal data that are listed in Article 9(2) GDPR, while rather the opposite should be the case.

ELI therefore recommends deleting Article 10(5) AI Act and inserting a significantly shortened and simplified ground for processing special categories of personal data in Article 9(2) GDPR (see below at III.3).

III. Amendments to the GDPR

1. Codifying the CJEU's judgment in *EDPS v SRB* (C-413/23 P)

The Digital Omnibus Proposal suggests codifying the judgment of the CJEU in C-413/23 P – *EDPS v SRB* by amending the definition of 'personal data' in Article 4(1) GDPR, inserting the words [emphasis added]

'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'

While ELI largely endorses the Commission's effort to clarify, within the GDPR itself, the potentially far-reaching consequences of this judgment, it considers that aspects of COM(2025) 837 final diverge from the CJEU's intended meaning.¹ In paragraph (85) of its judgment, the CJEU stated [emphasis added].

'Consequently, ... the EDPS is incorrect in so far as he submits that the fact that pseudonymised data are not, as the case may be, personal in nature for persons to whom the controller transfers the pseudonymised data makes it unduly possible to remove those data from the scope of EU law on the protection of personal data. According to that case-law, that fact has no bearing on the assessment of the personal nature of those data in the context, inter alia, of a potential

subsequent transfer of those data to third parties. Accordingly, in so far as it cannot be ruled out that those third parties have means reasonably allowing them to attribute pseudonymised data to the data subject, such as cross-checking with other data at their disposal, the data subject must be regarded as identifiable as regards both that transfer and any subsequent processing of those data by those third parties. In such circumstances, pseudonymised data should be considered to be personal in nature.'

The CJEU, therefore, clearly assumed that a party who is unable to identify the data subject by any reasonable means must still treat pseudonymised data as personal data as far as the subsequent transfer to third parties is concerned. The same must, for the sake of consistency, apply with regard to data security requirements.

Another aspect where ELI believes that COM(2025) 837 final is going too far concerns the role of mere legal prohibitions of re-identification. In Recital (27), we find the remark that data is anonymous for a party already where 'the identification of that data subject is prohibited by law', giving the example of the prohibition in Article 61(3) of Regulation (EU) 2025/327 concerning health data. ELI agrees that there may be situations where it is impossible for a party to identify the data subject because, due to institutional arrangements, the legal prohibitions are more or less fully enforced. However, this is certainly not the case with the majority of legal prohibitions.

ELI recommends the codifying of EDPS v SRB by re-drafting Article 4(1) in the following way (also streamlining and simplifying part of the existing definition):

¹ See also EDPB-EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), paragraphs 13, 16.

Article 4

Definitions

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, by a given entity, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because some other entity can identify the natural person. However, even where an entity does not have means reasonably allowing it to identify the natural person, pseudonymised data shall nevertheless be considered as personal data for that entity with regard, and limited to, the following:

- i. ensuring a level of security in line with Article 32 that is proportionate to the risk that an entity with means reasonably allowing it to identify the natural person gets access to the pseudonymised data;**
- ii. disclosure of the pseudonymised data to another entity where it cannot be ruled out that the other entity has means reasonably allowing it to identify the natural person; and**
- iii. disclosure of the pseudonymised data to another entity where it is to be reasonably expected that, ultimately, the data will be transferred to an entity that seeks to identify the natural person.**

Proposed accompanying Recitals:

This Regulation proposes a series of targeted amendments to Regulation (EU) 2016/679 for clarification and simplification, whilst preserving an adequate level of data protection. Article 4 of Regulation (EU) 2016/679 provides that personal data is any information relating to an identified or identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or

indirectly. Taking into account the case-law of the Court of Justice of the European Union concerning the definition of personal data (eg, Case C-413/23 P), it is necessary to provide further clarity on when a natural person should be considered to be identifiable. The existence of additional information enabling the data subject to be identified does not, in itself, mean that pseudonymised data must be regarded as constituting, in all cases and for every person or entity, personal data for the purposes of the application of Regulation (EU) 2016/679. In particular, it should be clarified that information is not to be considered personal data for a given entity where that entity does not have means reasonably likely to be used to identify the natural person to whom the information relates. The Commission, together with the European Data Protection Board, should support controllers in the application of this updated definition by stipulating technical criteria.

An entity for which the information is not personal data, in principle, does not fall within the scope of application of Regulation (EU) 2016/679. However, there have to be some restrictions for pseudonymised data, ie personal data that have undergone processing in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, which is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (point 5 of Article 4). For example, a company receiving pseudonymised health data from a hospital to assist in diagnostics may not have means reasonably allowing it to identify the individual patients, but still that company (which may be a processor, co-controller or independent controller) clearly cannot treat these health data as if they were fully anonymous weather data. Rather, that company is aware that the health data can be linked to the relevant individuals by any party who has the ‘key’, so it must bear this in mind when deciding on the appropriate level of data security measures. Likewise, when disclosing the data to third parties, the company must consider what the effect of that transfer will be and whether the third party may have the additional information required for identifying the individual patients. If this were the only restriction, it would still leave room for abusive practices where a first party

that does not have the means to identify the data subject passes pseudonymised data on to a second party (in particular a second party outside the Union) that does not have the means to identify the data subject either, but where the first party can, in the circumstances, reasonably expect that the second party will pass the data on to a third party and that this third party (or any other party further down the stream) has the key and will seek to identify the data subject. This is why the revised Article 4(1) clarifies that, also in this situation, the data is considered to be personal data already for the first party in the context of, and limited to, any transfer or disclosure.

2. Creating legal certainty for AI development and operation

The Digital Omnibus includes a number of proposals as to how data protection law can better support the development of AI in Europe. Among others, the Commission proposes inserting a new Article 88c GDPR on 'Processing in the context of the development and operation of AI'. The proposed new provision reads as follows:

'Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimisation during the stage of selection of sources and the training and testing of AI

an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.'

As far as special categories of personal data are concerned, a new point (k) is proposed to be inserted in paragraph 2, and a new paragraph 5 added. The wording proposed in the Digital Omnibus is as follows:

'2. ... (k) processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.

5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.'

A more technology-neutral solution that addresses the most salient points

ELI endorses these proposals in principle, but would like to draw attention to the following issues that seem to accompany the proposed solution:

- It is inconsistent that the AI-specific provision concerning Article 6 is placed in Article 88c, while the AI-specific provision concerning Article 9 is placed in Article 9 itself – for the sake of simplification, a consistent approach should be taken.

- The definition of an AI system in Article 3(1) of the AI Act is highly unclear² and potentially very narrow,³ which means that there may be uncertainty (and, in the worst case, an *argumentum e contrario*) for innovative technologies not falling within the definition: in the interest of innovation, a broader scope may therefore be more appropriate.
- The problem in practice is not so much uncertainty as to whether AI development can be a legitimate interest – the EDPB has already stated that this is the case⁴. Rather, the issue is that it is impossible to do a balancing test for each and every data point, plus, that there is massive uncertainty with regard to data subject rights where personal data seem to have been ‘memorised’.
- It is unclear what ‘protection against non-disclosure of residually retained data’ in the proposed Article 88c means. Possibly, it should read ‘protection against disclosure’, which would make more sense. However, it might also be understood as saying that filters, which prevent residually retained data in the model from being included in the output, are prohibited, which might not be a good policy choice.
- An ‘unconditional’ right to object to the processing of personal data may not be justified – this would override the provision in Article 21(1) according to which, after the data subject has objected to the processing, the controller may still demonstrate ‘compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims’. It may be preferable to rely on Article 21 as it stands.
- Likewise, it may not always be appropriate to oblige the controller to remove special

categories of data, as the processing of such data may be justified by another ground listed in Article 9(2).

- The new ground introduced by the proposed Article 9(2)(k) appears to be completely undermined by the proposed Article 9(5) as, ultimately, special categories of data must never be used for the training of AI, and it is even unclear from the drafting whether that excludes even explicit consent.

ELI still believes that a more technology-neutral solution which also addresses both the problem of large and heterogenous training data sets and the problem of what data subject rights mean for aggregated data in the model would be preferable. If that solution were to be integrated in a new Article 88c, and combined with elements proposed in COM(2025) 837 final, it could be phrased as follows:

Article 88c

Processing in the context of AI and similar technologies

1. **Processing of personal data for the development, provision, or use of technical solutions based on aggregated data, including AI systems or models, shall be deemed to be in conformity with this Regulation, where all of the following requirements are met:**
 - a. **the development, provision or use as such serves a legitimate interest pursued by the controller or by a third party, and such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects which require protection of personal data; and**

² ELI, The concept of ‘AI system’ under the new AI Act: Arguing for a Three-Factor Approach, 2024.

³ According to the Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5053 final, it may even exclude many systems developed by way of machine learning, see paras 42 ff.

⁴ EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, paras 59 ff.

- b. **appropriate safeguards, such as privacy-preserving upstream technical and organisational measures, have been applied which ensure that**
 - i. **it is not possible to re-identify the data subjects from the resulting system or model with any means reasonably likely to be used, except where there is a legal ground in Article 6(1) and, where relevant, Article 9(2); and**
 - ii. **the principles set forth in Article 5 are complied with to a degree that is reasonable in the circumstances, in particular the principle of lawfulness, fairness, and transparency.**

2. Where, despite the implementation of appropriate safeguards within the meaning of point b of paragraph 1, the controller learns of any personal data for whose processing there is no legal ground in Article 6(1) and, where relevant, Article 9(2), the controller shall remove such data. This applies to personal data at every stage of the lifecycle of the system or model, including to training, validation and testing data as well as input and output data.

3. If removal of relevant personal data within the meaning of paragraph 2, or compliance with any of the rights under Articles 16 to 18, 20 and 21 exercised by a data subject, requires effort that is disproportionate, the controller shall in any event

- a. **without undue delay implement appropriate safeguards, such as downstream technical and organisational measures, to prevent relevant personal data from being used or generated as output by the system or model; and**
- b. **remove the data or comply with any of the data subjects' rights as soon as this is possible with proportionate effort, such as upon the next major revision of the system or model.**

In determining proportionate effort, factors to be taken into account include the potential risk posed for data subjects, the efforts actually required and what they mean for the controller, the amount of investment made, and the compliance with data protection and other law in developing the technology, and the purposes for which the technology has been created.

4. Nothing in this Article shall be read as restricting the processing of personal data that would be permissible under other provisions of this Regulation.

Proposed accompanying Recitals:

A controller processing personal data for purposes that involve the processing of large and heterogeneous sets of data, including the training of AI models or systems with data collected from a variety of sources, may face significant difficulties in ensuring full compliance with Regulation 2016/679 for each individual data point. Likewise, once data are aggregated, removing traces of data points may prove to be extremely difficult and cause disproportionate effort. In order not to create a situation where such data activities can no longer be carried out in the Union, even if controllers have applied all reasonable and proportionate safeguards, the new Article 88c to be inserted in Regulation 2016/679 introduces a number of targeted simplifications for technical solutions that are based on aggregated data, including AI systems and models. To benefit from the privilege, a system or model need not qualify as an 'AI system' within the meaning of point 1 of Article 3 of Regulation 2024/1689, nor must any controller or processor assume any specific role defined therein, such as 'provider' or 'deployer'.

The new Article 88c provides that the development, provision or use of technical solutions that are based on aggregated data, including AI systems and models, shall be deemed to be in conformity with Regulation 2016/679 (including any requirements following from its Article 9) where the activity seen as a whole – ie, not necessarily at the level of the individual data point – is such as to satisfy the requirements set out for the legal basis of legitimate interests pursuant to Article 6(1), point (f), and appropriate safeguards are implemented. This implies that the development, provision, or use of AI will ordinarily constitute

a legitimate interest, subject to the purposes pursued and other relevant factors (for example, the development or use of an AI tool for fraudulent purposes would clearly not qualify for the privilege). Article 88c does not preclude reliance on other legal bases under Article 6 and, where applicable, Article 9 GDPR, such as the data subject's consent. However, to benefit from the privilege under Article 88c, the activity as a whole must satisfy the legitimate interests test.

The appropriate safeguards should ensure that it is not possible (in the sense of there being statistical guarantees that it is highly unlikely) to re-identify the data subjects from the resulting model with any means reasonably likely to be used, except where there is a legal ground in Article 6(1) and, where relevant, Article 9(2). They should also effectively operationalise the principles set out in Article 5, in particular the principle of lawfulness, fairness and transparency, taking into account the state-of-the-art and the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons. Such safeguards may include privacy-preserving 'upstream' technical and organisational measures, such as data governance and access controls, synthetic or anonymised data where appropriate, data minimisation and curation, pseudonymisation, federated or distributed learning, secure enclaves, differential privacy and robust security, as well as documentation, testing and human oversight. Although it is normally the provider's responsibility to implement these measures, also a deployer or other user of an AI system shall benefit from the privilege only where the AI system complies with these requirements, thereby encouraging the use of trustworthy and privacy-preserving systems.

The simplifications and clarifications provided by this Article apply across the entire lifecycle of AI systems and models, from data acquisition and collection, integration and preprocessing, through training, validation and testing, to deployment. Accordingly, any controller, including a provider or a deployer within the meaning of Regulation 2024/1689, may benefit from them. However, the requirement to implement appropriate safeguards is context-specific and will generally differ depending on whether the controller acts as a provider or as a deployer or user and, for providers, on the particular stage of the AI

lifecycle at which personal data are processed. For example, where a provider undertakes web scraping of data that are freely available on the internet, the controller can normally be expected to use available technology to anonymise or otherwise mitigate the processing of data that are manifestly personal, save where the personal data have been published in a manner that gives rise to a reasonable expectation that they have been manifestly made public by the data subject (such as entries on 'Wikipedia' and comparable sources). During model development, the provider can be expected to apply privacy-enhancing technologies that, to a degree reasonably achievable with state-of-the-art means, reduce the risk of the model memorising personal data. For a deployer or user, appropriate safeguards will include, for instance, applying model guardrails supplied by the provider and implementing organisational measures, such as access controls, logging, governance and procedures to handle data subject requests.

Even where appropriate safeguards have been implemented, it is still possible that controllers identify particular data points for which no legal ground under Article 6(1) and, where relevant, Article 9(2), exists. This may occur with regard to personal data at every stage of the lifecycle of an AI model, system, or other technical solution based on aggregated data, including the underlying inputs on which the aggregation relies, the risk of re-identification of those inputs from the model parameters, the generation of personal data through use of the model, the model itself, and the outputs. Where this is the case, the controller shall remove the relevant data. However, it is possible that, due to the technical characteristics of complex data pipelines or model architectures, immediate removal of such data would require disproportionate effort. In this case, controllers should, without undue delay, implement effective downstream technical and organisational measures (including, where relevant, providing downstream providers and deployers with such measures and ensuring, as far as reasonably possible, that they implement them) to prevent the use or generation as system output of the relevant data. They should also remove the data as soon as feasible with proportionate effort, for example at the next major revision or retraining cycle. Appropriate intervals between major revisions of the aggregated data model depend on the model's typical use, the

backlog of outstanding removals, and the quality of the interim solution, and should not impose efforts that are clearly disproportionate.

In determining what constitutes proportionate effort under this Regulation, a context-sensitive, risk-based assessment should be made, taking into account the potential risks to the rights and freedoms of data subjects, the actual efforts required and their organisational and financial implications for the controller (also considering the controller's size), the amount and nature of the investment made, compliance with data protection and other applicable law during development, and the purposes for which the technology has been created. This assessment should consider that models and systems may serve diverse purposes – such as scientific research, public interest tasks, or commercial deployment – and reflect the specific situation of open source development, noncommercial use, and micro-, small- and medium-sized enterprises (MSMEs), calibrating expectations to their capacities while ensuring that effective safeguards for data subjects are maintained. Generally, the efforts expected of providers of AI systems and models differ from those expected of mere deployers or other users, and the downstream technical and organisational measures required of each may vary substantially.

A very similar situation as with regard to the legal basis of processing may arise with regard to compliance with a data subject's rights under Articles 16 to 18, 20 and 21. Complying with the rights of data subjects under Regulation 2016/679 may pose a serious challenge where personal data have been aggregated in a way that, despite appropriate safeguards, they appear in the output, either because the model has 'memorised' personal data that was contained in the training data or because it produces information that is statistically plausible with respect to a natural person. For example, due to the opacity of AI models or systems, it may not be possible to provide access to or transfer the data in accordance with Articles 15 or 20 of Regulation 2016/679, or to erase the data in accordance with Article 17, for example where the data subject has exercised the right to object under Article 21. In such situations, complying with the full set of data subject rights under Regulation 2016/679 may involve disproportionate efforts or even be impossible without destroying the AI model or system. This is why, also in this

case, all that can reasonably be expected is that model guardrails (such as filter technologies) are implemented without undue delay and that the controller will fully comply with the data subject's request only when this becomes possible without disproportionate effort. In most scenarios, this will mean that data subject rights are suspended, in derogation of Article 12(5) GDPR.

Legal certainty regarding AI output and its relationship with the AI system or model

ELI would like to draw attention to the significant uncertainty that persists as to the conditions under which output referring to a natural person should be considered personal data, and if so, who should be considered as the controller. The difficulty arises from the fact that, even where no personal data originally relating to a data subject were used to train an AI model, generated output may resemble, and in fact be, personal data simply because the system may produce information that is statistically plausible with respect to the person.

A further point of uncertainty is whether there are rights and obligations following from the GDPR only with regard to output that is actually generated or also with regard to the relevant AI system or model itself.

ELI therefore suggests creating legal certainty regarding these issues. This could be achieved as follows:

Article 88d

Personal data in output

- 1. Whether or not a natural person's personal data were used in developing a technical solution based on aggregated data, including an AI system or model, any output is to be treated as personal data in respect of a natural person if it can reasonably be related to that identified or identifiable person.**
- 2. The party determining the purposes and means of processing the output, including by initiating its generation, using or storing it, shall be a controller of the personal data contained therein.**

3. **A provider, including a downstream provider, shall equally be considered as a controller with regard to the generation of output where**
 - a. **the output, or output containing similar personal data with regard to the data subject, is generated in a systematic manner; and**
 - b. **the information relating to the data subject was not provided by a downstream source beyond the control of the provider.**
4. **Where points a and b of paragraph 3 are fulfilled, a party controlling the system or model shall have the same obligations as that party would have if the generable output was processed as actual data under the control of that party.**

Proposed accompanying Recitals:

Significant uncertainty persists as to the conditions under which AI-generated output that refers to a natural person constitutes personal data within the meaning of point 1 of Article 4 of Regulation 2016/679. The uncertainty stems from the fact that, even where no personal data originally relating to that person were used to train the model, generated output may, in certain circumstances, relate to an identified or identifiable natural person. This should be held to be the case where the output can reasonably be attributed to that person, eg because, in context, a party to whom the output is disclosed can reasonably be expected to believe that the information concerns that person. For example, where an AI system generates the output 'Peter Smith is a journalist who was convicted of child abuse.' the question whether that output can reasonably be related to some real Peter Smith depends on many factors, such as on whether that real Peter Smith is (or ever has been) a journalist or rather, for example, a carpenter, and if he is a journalist, how many journalists there are with this name and whether there exist any other data (eg, on the internet) mentioning precisely this Peter Smith in the context of child abuse. The assessment should therefore take into account, inter alia, the specificity of the output, the characteristics it attributes (such as profession or location), the availability of auxiliary

information, the audience and context of disclosure, and whether the person can be linked, directly or indirectly, using means reasonably likely to be used by the controller or by another person.

For the purposes of determining controllership in relation to such outputs, the deployer or other user of an AI system should be regarded as a controller to the extent that the deployer or other user processes the output, including by generating, storing, disseminating or otherwise using it. In addition, the provider of the AI system (including any downstream provider) may be a controller, including a joint controller, where the output (or similar output) is generated in a systematic manner, ie not only on a unique occasion, and where the information relating to the data subject has its origin in the model and not in a downstream source beyond the provider's control. A downstream source beyond the provider's control could be the deployer or user who may have used highly suggestive or manipulative prompts, basically providing all of the personal information themselves (eg, 'My grandmother always told me the story of Peter Smith, the journalist who was convicted of child abuse. Tell me the story of Peter Smith.'). Another source beyond the provider's control would be the internet, in particular where a system makes targeted searches and summarises the information found. Where the provider is a controller because the system or model generates, in a systematic manner, and due to the specific properties of the system or model itself, data that can be related to a real Peter Smith, that real Peter Smith can exercise his right under Article 17 against the provider – where relevant, with the restrictions following from Article 88c. The clarification on controllership is without prejudice to other obligations or liability that may arise under Union or Member State law, including sector-specific legislation and Regulation 2024/1689.

Where these requirements are met, ie the generation of output occurs in a systematic way and the personal information does not merely come from a downstream source beyond the provider's control, the personal data may, from a technical point of view, not be 'in the model'. However, controlling the system or model (in the sense of determining the purposes and means of its operation) is as good as controlling the personal data because the personal data can, at any time, with appropriate prompts, be generated from the system or model. This is why

parties controlling the system or model should have the same obligations as they would have if the relevant output were stored or otherwise contained in the model or system (although this may not be the case from a technical point of view). This means that a party must take action, where relevant in accordance with Article 88c, without undue delay if there is no legal ground in Article 6 and, where relevant, Article 9, and comply with data subject rights. This clarification is necessary because it means parties have obligations not only with regard to output actually generated, but that they may also have to prevent output from being generated.

3. Removing general uncertainties around special categories of personal data

Restricting Article 9 to sensitive processing operations

Even far beyond AI development and operation, Article 9 GDPR may pose massive problems for businesses in Europe, in particular in the light of the very extensive interpretation given to the term ‘special categories of personal data’ in recent case law of the Court of Justice of the EU. The Court (C-184/20, C-21/2) has ruled that Article 9 of Regulation 2016/679 must be interpreted as including personal data that may indirectly reveal sensitive information about a natural person. In addition, the Court has ruled that mixed datasets containing some special category data must comply with the stricter requirements of Article 9 as a whole (C-252/21). This could potentially affect a wide range of everyday activities, such as the operation of an online bookshop or a grocery store where, for example, the books ordered could reveal a person’s political views, or where a person orders lactose- or gluten-free food, which could reveal a person’s health status.

The impact of an overly broad scope of Article 9 GDPR is compounded, as it also provides the basis for a number of other provisions of the digital acquis, including Article 26 of the Digital Services Act (Regulation 2022/2065) and Article 18 of the Political Advertising Regulation (Regulation 2024/900), as well as CJEU case law (eg, C 492/23 on obligations of platform providers).

In order to preserve the protective function of Article 9 of Regulation 2016/679 and to avoid an inflationary collection of ‘explicit consent’ for the most mundane activities, ELI believes that the provision should apply to the processing of sensitive personal data only where the biometric or genetic data allows the unique identification of a natural person or is inherently and specifically linked to sensitive characteristics. From a leaked early version of the Digital Omnibus Proposal, it appeared that the Commission had considered solving the ‘Article 9 problem’ in a more general manner but then changed its mind.

ELI urges the Commission to reconsider overcoming the massive uncertainties that come with Article 9 GDPR by replacing paragraph 1 of Article 9 by the following:

1. Insofar as the processing of personal data

- a. **concerns data that is biometric or genetic in nature and allows the unique identification of a natural person; or**
- b. **concerns data that is inherently and specifically linked with a natural person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation (‘sensitive characteristics’); or**
- c. **is for a purpose that is related to sensitive characteristics, in particular to record or infer sensitive characteristics or apply any differential treatment based on sensitive characteristics,**

such processing shall be lawful only if, and to the extent that, at least one of the cases in paragraph 2 applies.

In Article 9 paragraph 2 the words ‘Paragraph 1 shall not apply if’ must then be replaced by ‘Processing of personal data within the meaning of paragraph 1 is lawful if’. Paragraph 4 of Article 9 must be deleted, and in paragraph 3 the words ‘Personal data referred to in paragraph 1 may be processed for’ shall be replaced by ‘Processing of personal data referred to in paragraph 1 may occur for’.

Proposed accompanying Recitals:

Article 9 of Regulation (EU) 2016/679 currently prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. Article 9(2) provides narrowly framed exceptions, and Member States may add further conditions or limitations, particularly for genetic, biometric, or health data. In light of recent case law of the Court of Justice, the concept of 'special categories of personal data' appears to be interpreted very broadly, and mixed datasets may need to be treated under the special regime of Article 9. This could result in a large proportion of personal data being classified as special category data, with potentially paralysing effects on data use in Europe and prompting widespread reliance on 'explicit consent' for routine activities. To mitigate these consequences, Article 9 should apply to the processing of sensitive personal data only where biometric or genetic data enable the unique identification of a natural person or where the data are inherently and specifically linked to sensitive characteristics. This condition is clearly met for health records, but not for a holiday photograph that incidentally reveals a person's state of health (for instance, because the person wears glasses or uses crutches). Article 9 should also apply when data are processed for a purpose related to sensitive characteristics, in particular to infer such characteristics or to apply differential treatment based on them. By contrast, where data that could potentially reveal sensitive characteristics are used for purposes unrelated to such characteristics – such as performing a sales contract or conducting an indiscriminate analysis of large datasets to train a generalpurpose AI model – Article 9 should not apply.

Additional grounds for the permitted processing of special categories of personal data

In the Digital Omnibus Proposal, the Commission proposes adding a new ground for processing special categories of personal data in the context of biometric

verification (apart from the new ground related to AI, on which see above at 2):

'(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.'

ELI endorses this proposal, but would like to reiterate its proposal to add two more grounds to Article 9(2) GDPR, one with regard to performance of a contract and the other with regard to bias detection and correction. The latter is particularly important in order to avoid discrimination on a broad scale across different activities and technologies, including any AI. ELI believes that avoiding discrimination is sufficiently important for this new ground to be phrased along the lines of the other grounds so far listed in Article 9(2), and not along the lines of the proposed new Article 4a AI Act, which gives the impression that bias detection and mitigation pose a much higher risk to fundamental rights than other activities listed in Article 9(2) AI Act – while rather the opposite may be the case (see above at II.2).

ELI would also like to draw attention to the fact that it may be advisable to align the definition of 'biometric data' in the GDPR to the more recent definition in point 34 of Article 3 AI Act, and that, if the proposals made in COM(2025) 837 final are adopted, it may be advisable to include a definition of 'biometric verification'.

ELI therefore proposes to add also the following points k and m:

- k. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;**
- l. *[see Digital Omnibus proposal]***
- m. processing is necessary for detecting and correcting biases or avoiding discrimination and adequate safeguards are in place to prevent any use of the data for other purposes up to the point when the data are irreversibly anonymised or erased.**

Proposed accompanying Recitals:

Article 9(2) of Regulation 2016/679 previously failed to allow the processing of special categories of personal data in cases where such processing was necessary for the performance of a contract to which the data subject was a party, or for taking steps at the request of the data subject prior to entering into a contract. This meant that explicit consent had to be given for many day-to-day activities, even when the data subject had deliberately and knowingly entered into a contract involving the processing of special categories of data (eg health data), creating an unnecessary administrative burden and causing uncertainty. For this reason, this legal basis, with the strict interpretation given to it in the context of Article 6(1)(b), has been added to Article 9(2).

AI and related technologies have the potential to discriminate, including on the basis of sensitive characteristics, many of which are also protected characteristics under Union or Member State anti-discrimination law. It is therefore essential that such technologies are designed to avoid discrimination and that appropriate measures are taken at the design stage. This may require the processing of sensitive data, where the use of synthetic or anonymous data is not sufficient. While Article 10(5) of Regulation 2024/1689 has made this possible under certain conditions, the scope of the provision is limited to high-risk AI systems as defined in Regulation 2024/1689. However, the need to avoid bias and discrimination is not limited to high-risk AI systems. Therefore, Article 9 of Regulation 2016/679 should also not apply to the processing of sensitive personal data where the processing is carried out for the sole purpose of detecting and correcting bias or avoiding discrimination, provided that the processing of sensitive personal data is necessary for this purpose and that appropriate safeguards are in place to prevent any use of the data for other purposes, until such time as the data are irreversibly anonymised or erased. As this new provision is broader in scope than Article 10(5) of Regulation 2024/1689, the latter can be deleted.

IV. Consolidation of four legal instruments into a Data Act 2.0

With regard to the consolidation of the Data Act, DGA, FFDR and ODD into one single document, ELI would like to draw attention to the fact that it may not be appropriate to transfer all surviving provisions into the existing Data Act, given that this results in a patchwork that may be even more difficult for businesses to understand and comply with than the original legal instruments. Therefore, ELI would like to reiterate (see already above at I.3) that true simplification of the data-related acquis would require a fully redrafted new legal instrument, which could be a 'Data Economy Act', or an entirely new 'Data Act' that replaces the current one.

What ELI can do in the limited timeframe available for this consultation and considering what can realistically still be taken on board during the ongoing legislative procedure of the Digital Omnibus, ELI confines itself to a number of 'crunch points' that create particularly serious problems in practice.

1. Most urgent revisions in Chapter I

Scope of the Data Act

Article 1 Data Act on subject matter and scope has always been problematic because it combines very different aspects in one single Article. With the new additions proposed in COM(2025) 837, the length and complexity of the provision are still increased, while none of the shortcomings are really addressed. These shortcomings include the following:

Paragraph 1:

- Could be streamlined and simplified, in particular as the list is not in any way exhaustive.

Paragraph 2:

- The list of data covered by the various Chapters is not only superfluous, but also misleading because of the overlap and friction with the

individual provisions on scope that can be found in the majority of the Chapters.

- The message that Chapter II does not cover content is particularly misleading: as far as this excludes, eg, videos created with the help of a smartphone, such videos would not fall under the definition of product data or related services data anyway; however, the message could be misread as excluding also, eg, audio and video data recorded by the sensors of a connected vehicle, which is not the intention.
- Paragraph 2 can therefore be reduced to the important message that the Data Act covers personal and non-personal data, and this message should, for the sake of simplification and transparency, be merged with the message of current paragraph 5.

Paragraph 3:

- The provision on international scope, as it currently stands, suffers from several serious shortcomings, which could manifestly harm the interests of European businesses and create loopholes for businesses in third countries.
 - For example, data holders in third countries (eg, a Chinese car manufacturer) are captured only as far as they 'make data available to data recipients in the Union'. This is a nonsensical criterion – first, because a data holder in a third country can escape application of the Data Act simply by refusing to share data with data recipients in the Union, and, second, because this does not capture the important restrictions in Article 4(13) and (14), ie a Chinese car manufacturer can continue using non-personal data as they deem fit whereas all European car manufacturers had to stop using such data on 12 September 2025 or try to conclude an agreement.

- Another example is that data recipients are captured only insofar as they are ‘in the Union’. However, there is no provision that would hinder a user from requesting that data is made available to a data recipient outside the Union (although the data holder may not be under an obligation to comply with the request). This means that a European data recipient must comply with any restrictions following from the Data Act, while a Chinese data recipient is free to use the data made available to them as they deem fit.

- COM(2025) 837 final fails to add provisions on international scope with regard to the new Chapters added to the Data Act, ie the Chapters integrating provisions from the former DGA, ODD and FFDR.

Paragraph 4:

- This should not be in a provision on the scope of the Data Act, but (if it is needed at all) in the definition of connected product and related services; arguably, it creates more confusion than clarity, as a virtual assistant embedded in specific hardware is a connected product in its own right, while a virtual assistant that otherwise interacts with a connected product or related service is a related service in its own right.

Paragraph 5:

- This paragraph is redundant and could be shortened and integrated in (a drastically simplified) paragraph 2 for the sake of further simplification.

Paragraph 6:

- This paragraph is not only superfluous as its message is self-evident, but it is also misleading as it might give rise to an *argumentum e contrario* – it should be deleted, which would also serve the goal of further simplification.

Paragraph 7:

- COM(2025) 837 final proposes the deletion of this paragraph – ELI agrees.

Paragraph 8:

- The message of this paragraph is either superfluous (because it is self-evident) or

manifestly incorrect (because Chapter X does affect the *sui generis* right provided for in Article 7 of Directive 96/9/EC) – the paragraph should therefore be deleted.

Paragraph 9:

- This paragraph is helpful, but the selection of consumer protection legislation that is explicitly mentioned may not be ideal as, for example, overlap and potential friction with Directive 2011/83/EU is much less likely than overlap and potential friction with Directives (EU) 2019/770 or 2019/771 – ultimately, the only piece of legislation that really has to be mentioned in this paragraph for the sake of clarity is Directive 93/13/EEC (because of its complementarity with Chapter IV).

Paragraph 10:

- The message of this paragraph is self-evident, and the paragraph is therefore, at best, superfluous and should be deleted.

Proposed new paragraphs 11, 12 and 13 could be maintained, but would become paragraphs 6, 7 and 8.

For all these reasons, ELI recommends fully re-drafting Article 1 along the lines of the following:

Article 1

Subject matter and scope

- 1. This Regulation lays down harmonised rules, inter alia, on:**
 - a. the making available of data by data holders to other businesses or to consumers;**
 - b. the making available of data by data holders to public sector or Union bodies, where there is an exceptional need in the public interest;**
 - c. facilitating switching between data processing services;**
 - d. safeguards against unlawful third-country access to data;**

- e. **voluntary registration of data intermediation services and of entities which collect and process data made available for altruistic purposes;**
 - f. **data localisation requirements within the Union;**
 - g. **the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data;**
 - h. **the development of interoperability standards for data to be accessed, transferred and used; and**
 - i. **the establishment of a European Data Innovation Board.**
2. **This Regulation covers personal and non-personal data, unless explicitly provided otherwise. This Regulation is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein.**
3. **This Regulation applies to:**
- a. **manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;**
 - b. **data holders within the meaning of Chapter II, irrespective of their place of establishment, of product data or related services data generated by connected products or related services as referred to in point (a);**
 - c. **users in the Union of connected products or related services as referred to in point (a);**
 - d. **data holders, irrespective of their place of establishment, that are obliged under other Union law to make data available to data recipients in the Union;**
- e. **data recipients to whom data are made available under this Regulation or other Union law;**
 - f. **public sector bodies of Member States or Union bodies;**
 - g. **providers of data intermediation services and of entities which collect and process data made available for altruistic purposes, irrespective of their place of establishment, providing services to customers in the Union;**
 - h. **providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union; and**
 - i. **participants in data spaces established under Union law or Member State law in accordance with Union law.**
4. **This Regulation does not affect Union or national legal acts providing for the sharing of, access to and the use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties, or for customs and taxation purposes, or international cooperation in these areas.**
- This Regulation does not apply to areas that fall outside the scope of Union law and in any event does not affect the competences of the Member States concerning public security, defence or national security, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and the maintenance of law and order.**
5. **This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, including**

Directive 93/13/EEC.

6. **Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public sector bodies, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.**
7. **Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.**
8. **With regards to data and documents in the scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation does not affect the possibility for Member States to adopt more detailed or stricter rules, provided that those rules allow for more extensive re-use of data and documents.'**

Definition of 'data holder'

The definition of 'data holder' in point 13 of Article 2 Data Act has always been one of the most problematic definitions in the Data Act, as it is entirely circular and because the way in which the reference to product and related services data is phrased seems to make little sense. In the context of Chapters II and III of the Data Act, this has led to massive uncertainty, which is why a revision of the definition is overdue. COM(2025) 837 final suggests replacing the definition with a new definition, but, very surprisingly, this new definition is identical with the current one:

'(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use or make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service;'

Upon closer examination, the current definition suffers not only from circularity and generally poor drafting, but also from a second issue arising from the proposed merger of four legal instruments. ELI wishes to draw attention to the fact that the term 'data holder' is already used – and defined and understood differently, namely in a much more general sense – in the DGA as well as in the Recitals of the ODD. If the Data Act, DGA, and ODD are to be merged, there are three principal options to ensure consistency:

- Align the definition of 'data holder' with the DGA and introduce a new concept for Chapter II of the Data Act (for example, 'data access controller'), replacing 'data holder' with this new term throughout Chapters I to IV; or
- Change the concept of 'data holder' for the purposes of the new provisions to be inserted into the Data Act that originate in the DGA; or
- Adopt an overarching definition of 'data holder' that accommodates both contexts, supplemented by a sub-definition tailored specifically for Chapter II.

In the interest of keeping revisions to a minimum, ELI recommends the third option, ie using the term 'data holder' in a more general manner while introducing, for the purposes of Chapter II of the Data Act, a more specific definition. This might be phrased as follows:

(13) 'data holder' with regard to certain data means a natural or legal person that, alone or jointly with others, determines the purposes and means of processing the data; it includes a controller within the meaning of Article 4, point (7), of Regulation (EU) 2016/679. For the purposes of Chapter II of this Regulation,

it specifically means a natural or legal person other than the user of a connected product or related service that has, due to the design of the connected product or related service, direct access to the connected product or related service in such a way as to enable that person to retrieve product data or related services data without the help of the user.

Proposed accompanying Recitals:

The definition of ‘data holder’ in Article 2, point (13), of Regulation (EU) 2023/2854 has proved circular and overly tied to the notion of related services, generating legal uncertainty in particular for the application of Chapters II and III. In view of the objective of this Regulation to streamline and align the Union’s data-sharing framework by bringing together several legal instruments, including the DGA and the ODD that rely on a broader understanding of ‘data holder’, it is necessary to introduce a more general notion of ‘data holder’ plus, for the purposes of Chapter II, a more specific notion tailored to connected products and related services. To ensure coherence with Union law on the protection of personal data, the general notion of ‘data holder’ should be inspired by the concept of ‘controller’ in Article 4, point (7), of Regulation (EU) 2016/679, and a ‘data holder’ should include a controller. In essence, a data holder means a natural or legal person that, alone or jointly with others, determines the purposes and means of processing data.

For the purposes of Chapter II, ‘data holder’ should specifically designate any natural or legal person, other than the user of a connected product or related service, that, due to the design of that product or related service (including embedded software or telemetry), has direct access to product and/or related services data enabling the retrieval of product data or related services data without the user’s intervention. Direct access should be understood as local or remote, continuous or on-demand access that is technically enabled by the design. Where several persons have such access, they may each qualify as data holders for the data they control. This new definition provides much greater certainty in the multiparty relationships that are common in practice – both on the manufacturer or provider side, where multiple suppliers, partners, or affiliated companies

may be involved, and on the user side, where complex, layered arrangements arise (for example, a company operating a fleet of connected vehicles and renting them to individual customers).

Simplification and revision of other definitions

While the revision of other definitions is not as urgent as with regard to ‘data holder’, ELI would like to point out that a thorough revision of the definitions more generally seems to be highly advisable. This concerns, for example, the definition of **‘data processing service’**, which fails to allow a clear delineation of the services captured by Chapter VI of the Data Act and those falling outside the scope. It is particularly essential to draw a line between services that are, by their very nature, cloud or edge services (such as Infrastructure-as-a-Service, IaaS), and content and services that happen to be provided with the help of cloud or edge technologies.

It might also be advisable to have a simpler definition of **‘data’** that is more in line with existing definitions in international soft law (eg: ‘any representation of information recorded in any machine-readable format suitable for automated processing’). The current definition, which refers to ‘digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording’ appears to be not only unnecessarily long and complicated, but also inconsistent from a logical point of view, as ‘act’, ‘fact’ and ‘information’ are not on the same conceptual level and because a ‘compilation of ... acts’ is certainly not, as such, data.

The definition of **‘digital assets’** is also unfortunate, not least as, in everyday parlance and other soft and hard law instruments (eg UNIDROIT DAPL Principles), the term ‘digital assets’ has a much more specific meaning and connotations that are not appropriate for the purposes of Chapter VI. For example, the existing definitions of ‘digital assets’ and ‘exportable data’ could be merged into a new definition of ‘customer’s data’ (for example, customer’s data could mean: (a) data, including any digital content, which the customer has entrusted to the data processing service provider, such as by inputting or uploading to the provider’s ICT infrastructure or generating on that infrastructure with the help of inputted or uploaded

data; and (b) data, including any metadata, about the customer's use of the data processing service, which the parties have agreed to be exportable or which the customer could reasonably expect to be exportable).

As far as new definitions introduced by the Digital Omnibus Proposal are concerned, ELI suggests slightly re-phrasing the definitions of 'permission' and 'access'. First, in the interest of simplification, 'permission' should be used as a generic term that includes consent to the processing of personal data – otherwise, the Data Act always has to introduce two parallel provisions, one for personal and one for non-personal data. Also, it is unusual to define 'access' to data as a form of 'use' of data – use requires access, but not every access amounts to use.

ELI therefore urges the EU legislator to revise the definitions in due course.

2. Most urgent revisions in Chapters II and III (mandatory data sharing)

Clarifying the data holder's right to refuse sharing data for trade secrets protection

The only amendment which the Digital Omnibus Proposal includes for Chapter II is a slight reformulation of Article 4(8) and 5(11) on the data holder's exceptional right to refuse the sharing of data. This was originally phrased as follows, eg in Article 4(8):

'8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product, and shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.'

COM(2025) 837 final now proposes the following formulation [emphasis added]:

'8. In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets or that the disclosure of trade secrets to the user 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, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.'

While ELI supports the Commission's effort to improve the protection of European trade secrets, in particular against unlawful disclosure to third countries, it believes that the proposed formulation is much too complicated and ambiguous, in particular as it is still unclear whether the pivotal point is that the agreed technical and organisational measures (TOM) are insufficient, or whether the point is the risk that the user might not apply the TOM – arguably, it must be the latter if we take the protection of European trade secrets seriously.

ELI therefore recommends a much clearer and more transparent phrasing that enhances trade secrets protection, along the lines of the following:

- 8. In exceptional circumstances, where the data holder is able to demonstrate that**
 - a. the data holder or, where they are not the same person, the trade secret holder is highly likely to suffer serious economic damage if the user fails to apply the technical or organisational measures**

agreed upon; or

- b. **the disclosure of trade secrets to the user 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,**

that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay.

Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.

Proposed accompanying Recitals:

[Recitals (13) and (14) of COM(2025) 837 final could largely remain as they are].

Replacing Article 4(13) and (14) by a separate provision on the data holder's use of data

Article 4(13) and (14) have always been some of the most unclear provisions of the Data Act, creating massive uncertainty for businesses.

- Both provisions are very unexpected in this place, as Article 4 primarily concerns the user's access right, placed between Article 3 on direct

access and Article 5 on portability in a trilateral setting. Unsurprisingly, the provisions are often overlooked.

- The provisions are restricted to non-personal data, creating a situation where non-personal data enjoy stronger protection than personal data. More importantly, they give rise to massive uncertainty for businesses because treating data as personal in the event of doubt is no longer a 'safe harbour', and businesses find themselves between Scylla and Charybdis – there should be one baseline regime under the Data Act, and the GDPR should apply 'on top' where data qualifies as personal data.
- The provisions are restricted to 'readily available data'. However, while this concept makes sense in the context of the data holder's data sharing obligations, it fails to make sense in the context of the data holder's right to use data. The restrictions must also apply to data which the data holder can access only with some difficulty.
- It is unclear whether the contractual agreement is subject to fairness control under Chapter IV or whether permitting the data holder's data use is the main obligation under the contract and therefore excluded from unfairness control.
- It is unclear what the situation is if there is no agreement, but certain data have to be used by the data holder because of legal requirements or because it is necessary for the functioning of the product or the provision of the service – arguably, there can be a tacit agreement, but this should be clarified.
- The message to be conveyed by paragraph (14) remains entirely in the obscure as it is already unclear which party is referred to (because 'their contract' could refer either to the data holder or to the third parties) and whether paragraph (14), due to the formulation 'fulfilment', is narrower than paragraph (13) – the Commission Recommendation on model contractual terms⁵

⁵ Draft Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts, Annex, pp. 17 ff.

treats both paragraphs in the same way, more or less reducing paragraph (14) to the data holder's obligation to bind third parties.

ELI therefore recommends replacing paragraphs 13 and 14 of Article 4 Data Act and inserting the following new Article 3a:

Article 3a

Use of product data and related services data by data holder

- 1. A data holder may use product data or related services data only as far as such use is**
 - a. necessary for the functioning of the connected product or for the provision of the related service to the user; or**
 - b. required by Union law or national law in accordance with Union law; or**
 - c. agreed in a contract between the data holder and the user, without prejudice to Chapter IV or national law implementing Directive 93/13/EEC.**
- 2. A data holder shall not use product or related services data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any manner that could undermine the commercial position of that user on the markets in which the user is active.**
- 3. As far as use of the data by the data holder in accordance with paragraphs 1 and 2 includes the disclosure of data to third parties, the data holder shall contractually bind those third parties to apply at least the same safeguards for the user's legitimate interests as the data holder has to apply and not to further share data received, unless explicitly agreed otherwise with the user.**
- 4. As far as the data is personal data, use of the data by the data holder must also comply with Regulation (EU) 2016/679.**

Proposed accompanying Recitals:

To enhance legal certainty and ensure the coherent application of Regulation (EU) 2023/2854, it is necessary to clarify the conditions under which data holders may use product data and related services data. Article 4(13) and 4(14) have proved difficult to interpret, in particular as regards their placement within Article 4 on user access rights, their restriction to non-personal data, the legal effects in the absence of an explicit agreement, the identification of the relevant contractual parties, and the relationship between the two provisions. To address these ambiguities and to provide a transparent and proportionate framework that is technologically neutral and consistent with Union law on data protection and contract fairness, those paragraphs should be deleted and replaced by a standalone Article 3a. That Article should confine use by the data holder to what is necessary for the functioning of the connected product or for the provision of the related service to the user, that which is required by Union law or by Member State law in accordance with Union law, or that which is agreed in a contract between the data holder and the user, without prejudice to Chapter IV of this Regulation and to national law implementing Council Directive 93/13/EEC.

Apart from removing ambiguities and clear errors in drafting, the new Article 3a would introduce two substantive changes: first, the provision is no longer restricted to non-personal data. In particular in the light of recent case law of the Court of Justice, it is becoming increasingly difficult for parties to classify personal data as clearly personal or clearly non-personal. In other contexts, treating data as personal data in a case of doubt has always been a 'safe harbour' for businesses, but, under Article 4(13) and 4(14) Data Act, this is not the case. In the interest of simplicity and certainty, there should be one baseline regime under the Data Act, and the GDPR should apply 'on top' where data qualifies as personal data. Second, use of the data to the extent that this is necessary for the functioning of the product or the provision of the related service or as far as required by Union or national law in accordance with Union law, no longer requires an agreement. This means that data holders no longer need to worry whether, under the applicable contract law, a court would identify a tacit agreement to that end.

Eliminating errors and ambiguities by re-drafting Articles 7, 8, 11 and 12

Chapters II and III of the Data Act as they currently stand are not well drafted, and most of the Articles include provisions whose wording is unclear, redundant, misleading or even obviously inconsistent with what seems to have been the legislator's intention. While, to avoid disruption for businesses that have already started complying with the Data Act, major editorial changes should be avoided, cautious re-drafting of Articles 7, 8, 11 and 12 appears to be both necessary and practicable in order to create more legal certainty for businesses in Europe.

Article 7:

- It is currently unclear which obligations of whom shall not apply (eg, should the exception for products manufactured and services provided by SMEs really capture also the obligations following from Article 4(13) and (14) or Article 6 – arguably not).
- There is currently no exception for consumers re-selling or renting out connected products – this cannot be correct.
- The existing Article 7(2) creates massive problems in practice because it might be read as reducing party autonomy to almost zero, which undermines the governance approach of regulation-by-contract and is also inconsistent with Recital 25 and the Commission Recommendation on model contractual terms.⁶ It might be preferable to accept non-material derogations by the parties, and also derogations that are, in the light of any compensation provided, not to the detriment of the user.

Articles 8 and 12:

- There is massive overlap between both provisions – arguably, issues dealt with under Article 12 should be integrated in Article 8.

- The definition of the scope of Chapter III in Article 12(1) is obviously incorrect because the existing Articles 10 and 11 apply also where a data holder makes data available to a user.
- Several other provisions are misleading or even manifestly incorrect, eg the second part of Article 8(2) and Article 12(2) create the same problems and inconsistencies as Article 7(2); Article 8(4) is obviously incorrect as there are many other situations beyond a request by the user when a data holder may make data available to data recipients; Article 8(5) is much too general and arguably wrong in a number of situations.
- Several paragraphs in Article 8 are redundant, eg application of Chapter IV is referred to both in paragraph 1 and in paragraph 2, and non-discrimination is referred to both in paragraph 1 and in paragraph 3.

Article 11:

- The heading is incorrect as only the first paragraph concerns technical safeguards, while the other paragraphs address remedies for infringements – this should be split into two different Articles.
- The drafting is very complex and confusing, and there are several inconsistencies concerning who has which remedies against whom.
- There is a drafting error in point b of paragraph 2, as it should read 'and' instead of 'or'.
- It is unclear whether the list of remedies is exhaustive, which creates massive uncertainty and potential friction with applicable contract law.

ELI therefore recommends redrafting Articles 7, 8, 11 and 12, including by adding a new Article 11a and deleting current Article 12, while aiming to avoid substantive changes as far as possible, for example along the lines of the following:

⁶ Draft Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts, Annex, p. 32.

Article 7

Scope of obligations and restrictions under this Chapter

1. The obligations under Articles 3, 4 and 5 of this Chapter shall not apply to data generated through the use of connected products manufactured or designed or related services provided by
 - a. a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service; or
 - b. an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.
2. The obligations under paragraphs 2 and 3 of Article 3 shall not apply to a seller, rentor or lessor who is a person acting in a private and non-commercial capacity.

Article 8

Conditions under which data holders make data available

1. This Chapter shall apply where, in business-to-business relations, a data holder is obliged under Articles 4 or 5 or under applicable Union law or national legislation adopted in accordance with Union law, to make data available to a user or a data recipient.
2. Where, in business-to-business relations, a data holder is obliged to make data available to a data recipient under Article 5 or under

other applicable Union law or national legislation adopted in accordance with Union law, it shall agree with a data recipient the arrangements for making the data available and shall do so under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner in accordance with this Chapter and Chapters II and IV.

3. The contract shall not derogate, to the detriment of the user or the data recipient, from the rights and obligations under Chapter II and this Chapter or under relevant Union law or national legislation adopted in accordance with Union law in any material way, and such material derogation shall not be binding on the user or data recipient.

Where the data holder and the user or data recipient agree to modify or restrict certain rights or obligations, in particular the user's right to disclose data it has received under Article 4 to a third party, such modification or restriction shall not be considered to be material where it is not to the detriment of the user or data recipient, taking into account any adequate compensation.

4. Unless otherwise provided for in Union law, including Article 4(6) and Article 5(9) of this Regulation, or by national legislation adopted in accordance with Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets.

Article 11

Technical protection measures

1. A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with this Regulation as well as with the agreed contractual terms for making data available.
2. Technical protection measures shall not be used to circumvent obligations following from this Regulation or other Union law or national legislation adopted in accordance

with Union law, such as by discriminating between data recipients or hindering a user or third party from exercising their rights.

3. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.

Article 11a

Remedies in the case of infringements

1. The data holder and, where applicable and where they are not the same person, the trade secret holder, shall have the remedies listed in paragraph 2 where a data recipient, a user or any third party that has received data from a data recipient or a user has committed any of the following infringements:
 - a. for the purposes of obtaining data, provided false information, deployed deceptive or coercive means or abused gaps in technical infrastructure designed to protect the data;
 - b. used the data made available for unauthorised purposes, including the development of a competing connected product within the meaning of Article 6(2), point (e);
 - c. unlawfully disclosed data to another party;
 - d. not maintained the technical and organisational measures agreed pursuant to Articles 4(6) or 5(9); or
 - e. altered or removed technical protection measures applied by the data holder pursuant to Article 11 without the agreement of the data holder.
2. The infringing party shall comply, without undue delay, with the requests of the data

The user shall have the same remedies where the data recipient or any third party that has received data from a data recipient infringes Article 6(2), point (a) or (b).

2. The infringing party shall comply, without undue delay, with the requests of the data

holder and, where applicable and where they are not the same person, the trade secret holder or the user:

- a. to erase the data made available by the data holder and any copies thereof;
- b. to end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where
 - i. there is a serious risk that the unlawful use of those data will cause significant harm to the data holder, the trade secret holder or the user; and
 - ii. such a measure would not be disproportionate in light of the interests of the data holder, the trade secret holder or the user;
- c. to inform the user of the unauthorised use or disclosure of the data and of the measures taken to put an end to the unauthorised use or disclosure of the data;
- d. to compensate the party suffering from the misuse or disclosure of such unlawfully accessed or used data.

3. The remedies listed in paragraph 2 are without prejudice to remedies that follow from other Union law or national legislation adopted in accordance with Union law, including contract law, tort law and unfair competition law, or from contractual provisions agreed in accordance with this Chapter and Chapters II and IV.

Proposed accompanying Recital:

In order to enhance legal certainty and ensure coherent application of Chapters II and III of Regulation (EU) 2023/2854 without disrupting compliance efforts already undertaken by businesses, it is appropriate

to make targeted clarifications to Articles 7, 8, 11 and 12. These amendments are strictly editorial and structural in nature and do not alter the underlying policy choices. Article 7 should clearly delineate which obligations are subject to the micro-, small- and medium-sized enterprise exemptions, and introduce an explicit exception for private, noncommercial resale or rental of connected products, thereby avoiding undue burdens on consumers. Articles 8 and 12 should be streamlined and merged, removing uncertainties and redundancies. Article 8 should clarify, in line with Recital 25, that party autonomy remains a core feature of the contractual governance model in Chapters II and III, allowing the data holder and the user or data recipient to agree modifications that are not material, in particular where modifications are not to the detriment of the user, taking into account proportionate compensation, as is mentioned in Recital 25. Article 11 should focus on technical protection measures, while remedies for infringements should be set out in a separate Article 12, clearly identifying the parties entitled to seek erasure, cessation measures, information and compensation where a data recipient, user or downstream third party obtains data by deceptive or abusive means, misuses or unlawfully discloses data, fails to maintain agreed safeguards or tampers with technical protection measures.

3. Most urgent revisions in Chapter VI (cloud switching)

A simpler regulatory technique and more legal certainty concerning customer rights

Although it is one of the core provisions of Chapter VI, Article 25 of the Data Act presents stakeholders with a range of challenges, stemming partly from an unusual regulatory technique and partly from complex and opaque drafting.

As regards regulatory technique, Article 25 primarily imposes an obligation to conclude a contract while simultaneously prescribing its mandatory content at a level of granularity that leaves virtually no room for party autonomy. This approach of 'regulation-by-contract' has several serious drawbacks:

- It significantly increases transaction costs (cf.

the analogous situation under Article 28 GDPR), because for every contract falling within Chapter VI, the parties must ensure that all elements listed in Article 25 are included.

- It exacerbates the problem created by the vagueness of 'data processing service' (see above, p. 27), since parties need certainty about whether Chapter VI applies when drafting their contract.
- It creates uncertainty about the consequences of non-compliance: if parties fail to include the required provisions, it is unclear whether the terms in Article 25 apply directly, whether the customer has a claim for damages, or whether only administrative sanctions by the competent national authorities would follow.

In ELI's view, it would be preferable not to conflate, within a single article, the requirement to have a written contract with the customer's switching rights. Instead, one provision should set out the necessity of a written contract and the issues related to contract formation and party autonomy, while a separate provision should transparently delineate the customer's switching rights, including the switching timeline, as statutory rights.

In this context, it is worth noting that the current drafting of Article 25 makes it extremely difficult for stakeholders to understand the legislator's intended switching process.

- Provisions on timing are dispersed throughout the article, with cross-references in multiple directions and a proliferation of different concepts on timing – among them a 'mandatory maximum transitional period of 30 calendar days', a 'maximum notice period not exceeding two months', a 'retrieval period of at least 30 calendar days', a 'transitional period' and a period of '14 working days from the making of the switching request', plus potential 'alternative transitional' or 'alternative agreed' periods – some of which are combined in complex ways.
- It is also unclear whether the reference to 'a clause specifying that the contract shall be considered to be terminated' creates a separate termination right for the customer, and how this interacts

with termination rights under applicable contract law, including the consequences for remuneration due until the original end of the contract term.

ELI recommends that Article 25 be split into two Articles and redrafted in a much simpler and more transparent manner, with a coherent and consolidated timeline for switching and a clear delineation of contractual termination mechanics and their relationship to general contract law.

ELI therefore proposes to reorganise and clarify the provisions along the following lines [note that the terms 'digital assets' and 'exportable data' have been replaced by the term 'the customer's data']:

Article 25

Contractual terms concerning switching

1. **The rights of the customer and the obligations of the provider of data processing services in relation to switching between providers of such services or, where applicable, to an on-premises ICT infrastructure shall be clearly set out in a written contract. The provider of data processing services shall make that contract available to the customer prior to signing the contract in a way that allows the customer to store and reproduce the contract.**
2. **The contract shall not derogate, to the detriment of the customer, from the rights and obligations under this Chapter in any material way, and such material derogation shall not be binding on the customer.**

Article 25a

Customer rights concerning switching

1. **The customer has a right, at any time, to request the provider of data processing services to do any of the following, subject to any necessary cooperation on the part of the customer or the provider indicated by the customer:**
 - a. **port the customer's data to a different provider of data processing services indicated by the customer;**

- b. **port the customer's data to on-premises ICT infrastructure of the customer; or**
- c. **erase the customer's data.**

2. **The provider of data processing services must take action in accordance with the customer's request without undue delay. A switching and porting process must, in any event, be completed within a maximum transitional period not exceeding 30 calendar days after receiving the customer's request and, where relevant, expiry of any notice period that has been contractually agreed and that must not exceed two months.**

Where the mandatory maximum transitional period as provided for in subparagraph 1 is technically unfeasible, the provider shall notify the customer within 14 working days of receipt of the customer's request and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven months.

The customer has the right to extend the transitional period once for a period that the customer considers more appropriate for its own purposes.

3. **During the transitional period, the provider of data processing services shall:**
 - a. **provide reasonable assistance to the customer and third parties authorised by the customer in the switching process;**
 - b. **act with due care to maintain business continuity, and continue the provision of the functions or services under the contract;**
 - c. **support the customer's exit strategy relevant to the contracted services, such as by providing all relevant information, including information concerning known risks to continuity in the provision of the services on the source provider's own part; and**
 - d. **ensure that a high level of security is**

maintained throughout the switching process and during data transfer, insofar as security falls within the source provider's control, and ensure the continued security of the data for the duration of the retrieval period specified in paragraph 4.

- 4. The customer may request the contract to be terminated with effect from the successful completion of a switching and porting process or at any specific date thereafter, without prejudice to any other termination rights following from the contract or applicable law. From termination taking effect, the customer no longer has to pay the remuneration agreed, subject to any charges that have been contractually agreed and are consistent with Article 29. The customer may restrict termination to a separable part of the services where this is technically possible and agreed in the contract or allowed by applicable law.**

In the event of termination, the provider of data processing services shall:

- a. grant the customer an additional period for data retrieval of at least 30 calendar days from termination taking effect, unless the customer explicitly requests immediate erasure; and**
- b. guarantee full erasure of the customer's data, or the relevant part of the customer's data, after the expiry of the retrieval period referred to in point (a).**

Point (b) of the previous subparagraph does not prevent the data processing service provider from continuing to store the customer's data to the extent required by law or as far as is strictly necessary for the provider's or a third party's legitimate interests, such as the pursuit or defence of legal claims, unless those interests are overridden by the customer's legitimate interests to have the data erased.

Proposed accompanying Recitals:

In the interest of simplification and legal certainty, some largely editorial changes should be made to Chapter VI of Regulation (EU) 2023/2854. The relevant provisions should be streamlined by separating, within the original Article 25, contractual formation and transparency from statutory customer rights on switching. The current Article 25 conflates these elements and contains implicit rules on timelines and termination which are presented in a manner that is not always easy to follow and understand and whose relationship with national contract law is unclear. The amended framework therefore confines Article 25 to contractual terms concerning switching, requiring providers of data processing services to set out rights and obligations in a written contract that meets certain minimum standards, while introducing a new Article 25a that states the customer's statutory rights, applicable irrespective of contractual terms.

The new Article 25a should ensure effective switching by clarifying that customers have the right, at any time, to request the porting of all or part of their data to another provider or to on-premises ICT infrastructure, or the erasure of all or part of their data. It also includes clear and transparent rules about the relevant timelines, without introducing any substantive changes. During the transitional period, providers should give reasonable assistance to the customer and authorised third parties, maintain business continuity and the contracted functions, support the customer's exit strategy with relevant information including known continuity risks, and ensure a high level of security for data in transfer and during any retrieval period. The customer should be able to align termination with the successful completion of switching or any later date and, where technically feasible and permitted by the contract or applicable law, restrict termination to a separable part of the services.

A more transparent provision on charges

Similar observations apply to Article 29 on charges:

- Article 29 conflates transitional provisions – relevant only for a short period after the Data Act enters into force, and therefore better placed in Article 50 – with enduring provisions intended to govern future cases.

- Essential clarifications on the permissibility of early-termination penalties and sophisticated standard fee regimes appear only in Recital 89. Given their importance, they should be incorporated into the operative text, with explicit guidance on the conditions applicable to early termination penalties.
 - As drafted, Article 29 places all risks and costs on the provider even when switching is unusually difficult or expensive due to factors within the customer's or destination provider's sphere, such as untrained staff or inadequate ICT infrastructure – this cannot be correct.
- a. **not exceed the payments which would have become due at a minimum until the end of the contract period; and**
 - b. **adequately reflect any reduction, due to the early termination, in effort and expenses on the part of the provider.**
4. **Before entering into a contract with a customer, providers of data processing services shall provide the prospective customer with clear information on the standard service fees and early termination penalties that might be imposed.**

A more transparent provision could be obtained by revising Article 29 along the following lines:

Article 29

Charges in connection with switching and termination

1. **Providers of data processing services shall not impose any charges on the customer for the switching process.**

However, providers may charge customers for costs incurred that are directly linked to the switching process concerned as far as such costs exceed the costs which the provider could reasonably anticipate when concluding the contract because they are due to shortcomings in the sphere of the customer or the destination provider indicated by the customer, including failure to cooperate, lack of expertise or deficiencies in the ICT infrastructure.

2. **As far as compatible with other Union or Member State law, the contract may provide for a degressive calculation of standard service fees or any other benefit, such as loyalty rewards, which customers become entitled to after a certain contract period.**
3. **The contract may provide for fair and reasonable early termination penalties where the contract is for a fixed duration and the customer terminates the contract before the expiry of that duration. Such penalties must**

Where relevant, providers of data processing services shall provide information to a customer on data processing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.

5. **Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way.**
6. **The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by establishing a monitoring mechanism for the Commission to monitor the implementation of this Article.**

Proposed accompanying Recital:

In the interest of simplification, transparency and legal certainty, Article 29 of Regulation (EU) 2023/2854 should be refocused on charges applicable in all future cases, while the transitional provisions of limited temporal relevance should be moved to Article 50. In addition, the clarifications currently set out in Recital 89 concerning the permissibility of early termination penalties and standard fee regimes should be elevated into the operative text. In particular, the conditions for early termination penalties for fixed-term contracts terminated before expiry should be set out explicitly. Such penalties must be fair and reasonable, and they must not exceed the payments that would have fallen due at a minimum until the end

of the contract period, and duly reflect any reduction in the provider's effort and expenses resulting from early termination. As it would be unfair if the service provider also had to bear risks resulting from shortcomings in the customer's sphere, the revised Article 29 also establishes that the ban on switching charges is without prejudice to the recovery of costs directly linked to a specific switching process that exceed what was reasonably foreseeable at contract conclusion due to shortcomings in the sphere of the customer or of the destination provider indicated by the customer, including failure to cooperate, lack of expertise or deficiencies in ICT infrastructure. To support effective and consistent implementation, the Commission should remain empowered to adopt delegated acts establishing a monitoring mechanism for the application of this Article.

4. Most urgent revisions in Chapter XI

As currently drafted, Article 50 of the Data Act would have significant retroactive effects, which are further amplified by the requirement in Article 29 to apply reduced switching charges to a period preceding the Act's applicability. ELI questions whether this is compatible with EU primary law. The concern arises primarily in relation to Chapter VI, for which no transitional provisions are provided, but also with respect to Chapter II, where a transitional provision exists only for Article 3(1). However, it should be borne in mind that:

- Where manufacturers are not obliged to design their connected products in accordance with Article 3(1), they are unlikely to provide the information that sellers, renters, and lessors require from manufacturers to comply with Article 3(2).
- For connected products placed on the market before the Data Act entered into force, data holders had no reason to negotiate the agreements required by Article 4(13), establish the technical and organisational measures for data sharing, or set prices with future data-sharing obligations in mind.
- The same is true for cloud service providers,

who have not had an opportunity to renegotiate their contracts in light of the Data Act's rules on permissible and impermissible fee structures.

Regarding Chapter VI, COM(2025) 837 final attempts to solve the issue by inserting, in Article 31, new paragraphs 1a and 1b:

'1a. The obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025.

The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.

1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).

Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.

Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry 1 if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.'

ELI is not convinced that the new provisions resolve the issue:

- Both proposed provisions are drafted so intricately and ambiguously that their substance and underlying rationale are difficult to discern. Moreover, Article 31 is an inappropriate vehicle for what is essentially a transitional rule; such provisions should be consolidated in Article 50.
- Because the prohibition on switching charges remains applicable with full retroactive effect, the proposal does not address the challenges faced by providers – including major European businesses – who did not negotiate enhanced standard service fees or early-termination penalties due to uncertainty about the future legal framework.

ELI therefore proposes extending the transitional provision foreseen for Article 3(1) to the entirety of Chapter II, and applying the transitional provision foreseen for Chapter IV to Chapter VI [changes underlined]:

Article 50

Entry into force and application

- 1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.**

It shall apply from 12 September 2025.

- 2. Chapter II shall apply to connected products and the services related to them placed on the market after 12 September 2026.**
- 3. Chapter III shall apply in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which enters into force after 12 September 2025.**
- 4. Chapter IV and Chapter VI shall apply to contracts concluded after 12 September 2025.**

Chapter IV and Chapter VI shall apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are:

- a. of indefinite duration; or**
- b. due to expire at least 10 years from 11 January 2024.**

Proposed accompanying Recital:

To uphold the principles of legal certainty, legitimate expectation and nonretroactivity under Union law, the transitional framework of the Data Act should be clarified and reinforced. In particular, the concerns raised in relation to Chapter VI, including Article 29 on switching charges, and to Chapter II, where a transitional provision currently exists only for Article 3(1), warrant targeted adjustments to ensure prospective application and a reasonable adaptation period for existing contractual and technical arrangements. The transitional provision foreseen for Article 3(1) should be extended to the entirety of Chapter II, recognising that manufacturers of connected products to whom the design requirements under Article 3(1) do not apply will most likely not provide to sellers, renters or lessors the information they need for fulfilling their obligations under Article 3(2). Likewise, data holders will not have prepared for their extensive sharing obligations, and will not have implemented the agreements envisaged by Article 4(13) and (14). Regarding Chapter VI, the Data Act fails to provide for a transitional period, although providers have not had a chance to negotiate their contracts against the background of the fee structures that are permissible under the Data Act. The transitional provision foreseen for Chapter IV should therefore apply *mutatis mutandis* to Chapter VI.

ANNEX: Visualising proposed amendments to the Digital Omnibus

1. Redrafting that aims at substantive changes

AI Act

AI Act with amendments by Omnibus Proposal COM(2025) 836 final	Comments	ELI Proposal
<i>Article 4a Processing of special categories of personal data for bias detection and mitigation</i>		
<p>1. To the extent necessary to ensure bias detection and correction in relation to high-risk AI systems in accordance with Article 10 (2), points (f) and (g), of this Regulation, providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the safeguards set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable, all the following conditions shall be met in order for such processing to occur:</p>	<p>The provision on processing special categories of data should be moved to Article 9 GDPR and drafted consistently with the grounds listed in Article 9(2), see ELI proposal for a new Article 9(2) (m) GDPR.</p> <p>This would simplify the framework, enhance coherence, further incentivise bias detection and correction, and ensure that one and the same authority is competent, thereby promoting uniform application.</p>	
<p>a. the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;</p> <p>b. the special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation;</p>		

<p>c. the special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations;</p> <p>d. the special categories of personal data are not transmitted, transferred or otherwise accessed by other parties;</p> <p>e. the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;</p> <p>f. the records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was necessary to detect and correct biases, and why that objective could not be achieved by processing other data.</p> <p>2. Paragraph 1 may apply to providers and deployers of other AI systems and models and deployers of high-risk AI systems where necessary and proportionate if the processing occurs for the purposes set out therein and provided that the conditions set out under the safeguards set out in this paragraph.</p>		
<p><i>Article 113</i> Entry into force and application</p>		<p><i>Article 113</i> Entry into force and application</p>
<p>This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i>.</p> <p>It shall apply from 2 August 2026.</p>		<p>1. This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i>.</p> <p>2. It shall apply from 2 August 2026.</p>

<p>However:</p> <ul style="list-style-type: none"> a. Chapters I and II shall apply from 2 February 2025; b. Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101; 		<p>3. However:</p> <ul style="list-style-type: none"> a. Chapters I and II shall apply from 2 February 2025; b. Chapter III Section 4, Chapter V, Chapter VII and Chapter XII and Article 78 shall apply from 2 August 2025, with the exception of Article 101;
<ul style="list-style-type: none"> c. Article 6(1) and the corresponding obligations in this Regulation shall apply from 2 August 2027 	<p>If point c is retained, there is an inconsistency with point d. ii. Point c should therefore be deleted.</p>	
<p>d. Chapter III, Sections 1, 2, and 3, shall apply following the adoption of a decision of the Commission confirming that adequate measures in support of compliance with Chapter III are available, from the following dates:</p> <ul style="list-style-type: none"> i. 6 months after the adoption of that decision as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and ii. 12 months after the adoption of the decision as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I. <p>In the absence of the adoption of the decision within the meaning of subparagraph 1, or where the dates below are earlier than those that follow the adoption of that decision, Chapter III, Sections 1, 2, and 3, shall apply:</p> <ul style="list-style-type: none"> i. on 2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and ii. on 2 August 2028 as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I. 	<p>Making the date of application conditional upon a Commission decision is problematic as this produces uncertainty regarding the application of the Regulation’s provisions. This uncertainty is particularly detrimental as it concerns the application of Chapter III, Sections 1 to 3, which contain the core provisions of the AI Act. To ensure predictability and enable operators to plan compliance actions, ELI proposes fixed application dates.</p>	<ul style="list-style-type: none"> c. Chapter III, Sections 1, 2, and 3, shall apply i. on 2 December 2027 as regards AI systems classified as high-risk pursuant to Article 6(2) and Annex III, and ii. on 2 August 2028 as regards AI systems classified as high-risk pursuant to Article 6(1) and Annex I;
<ul style="list-style-type: none"> e. Articles 102 to 110 shall apply from [the date of entry into application of this Regulation]. 		<ul style="list-style-type: none"> d. Articles 102 to 110 shall apply from [the date of entry into application of the Digital Omnibus Regulation].

GDPR

<p>GDPR with amendments by Omnibus Proposal COM(2025) 837 final</p>	<p>Comments</p>	<p>ELI Proposal</p>
<p><i>Article 4 Definitions</i></p>		<p><i>Article 4 Definitions</i></p>
<p>1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.</p> <p>[...]</p>	<p>The wording proposed in COM(2025) 837 final fails to ensure consistency with the judgment of the CJEU in C-413/23 P – EDPS v SRB. A different wording should therefore be preferred that acknowledges remaining obligations with regard to pseudonymised data, in particular concerning data security and any transfer of the data to a third party.</p>	<p>1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by a given entity, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because some other entity can identify the natural person. However, even where an entity does not have means reasonably allowing it to identify the natural person, pseudonymised data shall nevertheless be considered as personal data for that entity with regard, and limited to, the following:</p> <ul style="list-style-type: none"> i. ensuring a level of security in line with Article 32 that is proportionate to the risk that an entity with means reasonably allowing it to identify the natural person gets access to the pseudonymised data; ii. disclosure of the pseudonymised data to another entity where it cannot be ruled out that the other entity has means reasonably allowing it to identify the natural person; and iii. disclosure of the pseudonymised data to another entity where it is to be reasonably expected that, ultimately, the data will be transferred to an entity that seeks to identify the natural person. <p>[...]</p>

<p><i>Article 9</i> Processing of special categories of personal data</p>		<p><i>Article 9</i> Processing of special categories of personal data</p>
<p>1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.</p>	<p>In the light of recent case law of the CJEU that interprets 'special categories of personal data' very broadly, Article 9 GDPR might have paralysing effects on data use in Europe and lead to inflationary use of 'explicit consent' for the most mundane processing activities.</p> <p>Article 9(1) GDPR should therefore be revised so as to reflect a more risk based approach, ie its application should be reduced to situations where sensitive characteristics are really at stake.</p>	<p>1. Insofar as the processing of personal data</p> <ul style="list-style-type: none"> a. concerns data that is biometric or genetic in nature and allows the unique identification of a natural person; or b. concerns data that is inherently and specifically linked with a natural person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation ('sensitive characteristics'); or c. is for a purpose that is related to sensitive characteristics, in particular to record or infer sensitive characteristics or apply any differential treatment based on sensitive characteristics, <p>such processing shall be lawful only if, and to the extent that, at least one of the cases in paragraph 2 applies.</p>
<p>2. Paragraph 1 shall not apply if one of the following applies: [...]</p>	<p>(Editorial redraft reflecting other changes proposed by ELI).</p>	<p>2. Processing of personal data within the meaning of paragraph 1 is lawful if one of the following applies: [...]</p>
<p><i>k. processing in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, subject to the conditions referred to in paragraph 5.</i></p>	<p>It is inconsistent that this AI-specific provision is inserted in Article 9, while it is proposed that the AI-specific provision on the legal basis for processing is integrated in a new Article 88c.</p> <p>Besides, point k. as proposed by COM(2025) 837 final is not convincing as the fact that processing occurs 'in the context of' an AI system can hardly serve as justification.</p>	
	<p>To avoid the soliciting of explicit consent for many day-to-day activities, even when the data subject deliberately and knowingly entered into a contract involving the processing of special categories of data, contractual necessity should be a ground listed in Article 9(2).</p>	<p>k. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;</p>

<p><i>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.</i></p>		<p>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.</p>
	<p>A streamlined and simplified version of Article 4a AI Act as proposed by COM(2025) 836 final should be inserted here.</p>	<p>m. processing is necessary for detecting and correcting biases or avoiding discrimination and adequate safeguards are in place to prevent any use of the data for other purposes up to the point when the data are irreversibly anonymised or erased.</p>
<p>3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) [...].</p>	<p>(Editorial redraft reflecting other changes proposed by ELI).</p>	<p>3. Processing of personal data referred to in paragraph 1 may occur for the purposes referred to in point (h) [...].</p>
<p>4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.</p>	<p>This provision should be deleted as it adds to the fragmentation of data protection law in the Union.</p>	
<p><i>5. For processing referred to in point (k) of paragraph 2, appropriate organisational and technical measures shall be implemented to avoid v the collection and otherwise processing of special categories of personal data. Where, despite the implementation of such measures, the controller identifies special categories of personal data in the datasets used for training, testing or validation or in the AI system or AI model, the controller shall remove such data. If removal of those data requires disproportionate effort, the controller shall in any event effectively protect without undue delay such data from being used to produce outputs, from being disclosed or otherwise made available to third parties.</i></p>	<p>All AI-specific provisions should be integrated in the proposed new Article 88c (plus a new Article 88d).</p> <p>Article 9(5) as drafted in COM(2025) 837 final effectively undermines the privilege granted by proposed Article 9(2)(k) because, ultimately, it seems to prohibit the use of special categories of data for the training of AI.</p> <p>Besides, 'effectively protect ... from being disclosed' might not be possible as sophisticated actors could analyse the model weights, in particular in the case of open source and open weight models.</p>	
<p><i>Article 88c Processing in the context of the development and operation of AI</i></p>	<p>This provision should be phrased and drafted in a more technology-neutral way.</p>	<p><i>Article 88c Processing in the context of AI and similar technologies</i></p>

<p>Where the processing of personal data is necessary for the interests of the controller in the context of the development and operation of an AI system as defined in Article 3, point (1), of Regulation (EU) 2024/1689 or an AI model, such processing may be pursued for legitimate interests within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, where appropriate, except where other Union or national laws explicitly require consent, and where such interests are overridden by the interests, or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.</p> <p>Any such processing shall be subject to appropriate organisational, technical measures and safeguards for the rights and freedoms of the data subject, such as to ensure respect of data minimization during the stage of selection of sources and the training and testing of AI an system or AI model, to protect against non-disclosure of residually retained data in the AI system or AI model to ensure enhanced transparency to data subjects and providing data subjects with an unconditional right to object to the processing of their personal data.</p>	<p>A more technology-neutral wording would foster innovation and increase legal certainty by eliminating doubts about the applicability of Article 88c, given that the definition of an AI system in Article 3(1) AI Act is highly unclear and potentially very narrow.</p> <p>The formulation should clarify that any test of legitimate interests is applied at the macro level of the entire activity of developing, providing, or using an AI system or model, and not at the granular level of the individual data point.</p> <p>In essence, the solution proposed by ELI would ensure that trustworthy AI systems that respect European values, including data protection, to the full extent that is reasonable in the circumstances enjoy a privilege.</p> <p>Needless to say, this is without prejudice to the controller relying on any other legal ground, such as consent.</p> <p>In terms of data subject rights, it may not be justified to grant an 'unconditional' right to object as this would override the 'compelling legitimate grounds' referred to in Article 21(1) GDPR.</p>	<ol style="list-style-type: none"> 1. Processing of personal data for the development, provision, or use of technical solutions based on aggregated data, including AI systems or models, shall be deemed to be in conformity with this Regulation, where all of the following requirements are met: <ol style="list-style-type: none"> a. the development, provision or use as such serves a legitimate interest pursued by the controller or by a third party, and such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects which require protection of personal data; and b. appropriate safeguards, such as privacy-preserving upstream technical and organisational measures, have been applied that ensure that <ol style="list-style-type: none"> i. it is not possible to re-identify the data subjects from the resulting system or model with any means reasonably likely to be used, except where there is a legal ground in Article 6(1) and, where relevant, Article 9(2); and ii. the principles set forth in Article 5 are complied with to a degree that is reasonable in the circumstances, in particular, the principle of lawfulness, fairness, and transparency.
	<p>An AI-specific provision, similar to that proposed by COM(2025) 837 final to be included in a new Article 9(5) GDPR, should be integrated in Article 88c. It should be generalised, ie be applied to all problems regarding a legal ground in Article 6 and/or, where relevant, Article 9(2).</p> <p>In essence, where an AI system enjoys the privilege, no disproportionate efforts have to be made even where, at a later point, the controller learns of data for which there is no legal ground.</p>	<ol style="list-style-type: none"> 2. Where, despite the implementation of appropriate safeguards within the meaning of point b of paragraph 1, the controller learns of any personal data for whose processing there is no legal ground in Article 6(1) and, where relevant, Article 9(2), the controller shall remove such data. This applies to personal data at every stage of the lifecycle of the system or model. 3. If removal of relevant personal data within the meaning of paragraph 2, or compliance with any of the rights under Articles 16 to 18, 20 and 21 exercised by a data subject requires effort that is disproportionate, the controller shall in any event

	<p>There should be a similar provision also with regard to data subject rights, which, in practice, may be the more difficult challenge anyway.</p>	<ul style="list-style-type: none"> a. without undue delay implement appropriate safeguards, such as downstream technical and organisational measures, to prevent relevant personal data from being used or generated as output by the system or model; and b. remove the data or comply with any of the data subjects' rights as soon as this is possible with proportionate effort, such as upon the next major revision of the system or model. <p>In determining proportionate effort, factors to be taken into account include the potential risk posed for data subjects, the efforts actually required and what they mean for the controller, the amount of investment made, and the compliance with data protection and other law in developing the technology, and the purposes for which the technology has been created.</p>
	<p>The privilege proposed by ELI does not restrict activities that are permitted under other provisions.</p>	<p>4. Nothing in this Article shall be read as restricting the processing of personal data that would be permissible under other provisions of this Regulation.</p>
	<p>A provision on system output would be desirable in the light of the degree of uncertainty associated with it.</p>	<p style="text-align: center;"><i>Article 88d</i> Personal data in output</p>
	<p>This is a clarification that system output can be qualified as personal data even where no personal data of the relevant data subject have been used for the training.</p>	<p>1. Whether or not a natural person's personal data were used in developing a technical solution based on aggregated data, including an AI system or model, any output is to be treated as personal data in respect of a natural person if it can reasonably be related to that identified or identifiable person.</p>
	<p>With regard to system output, we need to define who is the controller, in particular under what conditions it is exclusively the deployer or other user, or the deployer jointly with the provider.</p>	<ul style="list-style-type: none"> 2. The party determining the purposes and means of processing the output, including by initiating its generation, using or storing it, shall be a controller of the personal data contained therein. 3. A provider, including a downstream provider, shall equally be considered as a controller with regard to the generation of output where

		<ul style="list-style-type: none"> a. the output, or output containing similar personal data with regard to the data subject, is generated in a systematic manner; and b. the information relating to the data subject was not provided by a downstream source beyond the control of the provider.
	<p>Where the provider is the controller the personal data may, from a technical point of view, not be 'in the model'. However, a party controlling the system or model should have the same obligations as if they were, ie take action (in accordance with Article 88c) without undue delay if there is no legal ground in Article 6 and, where relevant, Article 9.</p>	<p>4. Where points a and b of paragraph 3 are fulfilled, a party controlling the system or model shall have the same obligations as that party would have if the generable output was processed as actual data under the control of that party.</p>

Data Act

Data Act with amendments by Omnibus Proposal COM(2025) 837 final	Comments	ELI Proposal
<p><i>Article 4</i> The rights and obligations of users and data holders with regard to access, use and making available product data and related service data</p>	<p>The placement of paras 13 and 14 of Article 4 is unexpected and they are often overlooked. ELI proposes replacing them with a standalone Article 3a.</p>	<p><i>Article 3a</i> Use of product data and related services data by data holder</p>
<p>[...] 13. A data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user.</p>	<p>Articles 4(13) and 4(14) have proved to be substantially unclear, difficult to interpret and suffering from several flaws in the drafting.</p> <p>With regard to the existing Article 4(13), several clarifications should be made to provisions that have proved to cause difficulties in practice (eg restriction to readily available data, processing of data in the absence of an agreement, subjection of an agreement to fairness control under Chapter IV).</p>	<ul style="list-style-type: none"> 1. A data holder may use product data or related services data only as far as such use is <ul style="list-style-type: none"> a. necessary for the functioning of the connected product or for the provision of the related service to the user; or b. required by Union law or Member State law in accordance with Union law; or c. agreed in a contract between the data holder and the user, without prejudice to Chapter IV or national law implementing Directive 93/13/EEC.

<p>A data holder shall not use such data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any other manner that could undermine the commercial position of that user on the markets in which the user is active.</p>		<p>2. A data holder shall not use product or related services data to derive insights about the economic situation, assets and production methods of, or the use by, the user in any manner that could undermine the commercial position of that user on the markets in which the user is active.</p>
<p>14. Data holders shall not make available non-personal product data to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them.</p>	<p>The meaning of the existing Article 4(14) is almost impossible to discern. The provision should be reduced to the parts that appear to make sense.</p>	<p>3. As far as use of the data by the data holder in accordance with paragraphs 1 and 2 includes the disclosure of data to third parties, the data holder shall contractually bind those third parties to apply at least the same safeguards for the user's legitimate interests as the data holder has to apply and not to further share data received, unless explicitly agreed otherwise with the user.</p>
	<p>The new Article 3a should apply to both non-personal and personal data, with the GDPR applying additionally with regard to personal data.</p>	<p>4. As far as the data is personal data, use of the data by the data holder must also comply with Regulation (EU) 2016/679.</p>
<p><i>Article 31</i> Specific regime for certain data processing services</p>		<p><i>Article 31</i> Specific regime for certain data processing services</p>
<p>1. The obligations laid down in Article 23, point (d), Article 29 and Article 30(1) and (3) shall not apply to data processing services [...]</p> <p>1a. The obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer, if the provision of such services is based on a contract concluded before or on 12 September 2025.</p> <p>The provider of such data processing services shall not be required to renegotiate or amend a contract for the provision of those services before its expiry if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.</p>	<p>Paragraphs 1a and 1b are difficult to interpret and essentially transitional provisions. They would, therefore, be better placed in Article 50.</p> <p>Ultimately, ELI proposes a different approach to Article 50, on which see below.</p>	<p>1. The obligations laid down in Article 23, point (d), Article 29 and Article 30(1) and (3) shall not apply to data processing services [...]</p>

<p>1b. A provider of a data processing service may include provisions on proportionate early termination penalties in a contract of fixed duration on the provision of data processing services other than those referred to in Article 30(1).</p> <p>Where the provider of data processing service is a small and medium-sized enterprise or a small mid-cap, the obligations laid down in Chapter VI, with the exception of Article 29, and in Article 34 shall not apply to data processing services other than those referred to in Article 30(1), if the provision of such services is based on a contract concluded before or on 12 September 2025.</p> <p>Where the provider of a data processing service is a small and medium-sized enterprise or a small mid-cap, the provider shall not be required to renegotiate or amend a contract for the provision of a data processing service other than those referred to in Article 30(1) before its expiry 1 if that contract was concluded before or on 12 September 2025. Any contractual provision contained in that contract that is contrary to Article 29(1), (2), or (3) shall be considered null and void.</p> <p>2. The obligations laid down in this Chapter shall not apply to data processing services [...]</p>		
<p><i>Article 50</i> Entry into force and application</p>		<p><i>Article 50</i> Entry into force and application</p>
<p>This Regulation shall enter into force on the twentieth day following that of its publication in the <i>Official Journal of the European Union</i>.</p> <p>It shall apply from 12 September 2025.</p>		<p>1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.</p> <p>It shall apply from 12 September 2025.</p>
<p>The obligation resulting from Article 3(1) shall apply to connected products and the services related to them placed on the market after 12 September 2026.</p>	<p>To avoid retroactive effects and ensure compatibility with primary law, the transitional provision for Article 3(1) in Article 50 should be extended to the whole of Chapter II.</p>	<p>2. Chapter II shall apply to connected products and the services related to them placed on the market after 12 September 2026.</p>

<p>Chapter III shall apply in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which enters into force after 12 September 2025.</p>		<p>3. Chapter III shall apply in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which enters into force after 12 September 2025.</p>
<p>Chapter IV shall apply to contracts concluded after 12 September 2025.</p> <p>Chapter IV shall apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are:</p> <ol style="list-style-type: none"> a. of indefinite duration; or b. due to expire at least 10 years from 11 January 2024 	<p>To avoid retroactive effects and ensure compatibility with primary law, the transitional provisions for Chapter VI in Article 50 should be extended to Chapter VI.</p>	<p>4. Chapter IV and Chapter VI shall apply to contracts concluded after 12 September 2025.</p> <p>Chapter IV and Chapter VI shall apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are:</p> <ol style="list-style-type: none"> a. of indefinite duration; or b. due to expire at least 10 years from 11 January 2024.

2. Editorial redrafting that eliminates errors, inconsistencies and ambiguities

The following table lists those ELI proposals that are of an editorial or clarificatory nature and do not intend to affect any policy choices. Accordingly, they may not require further political deliberation. That said, where provisions are so unclear that their meaning cannot be discerned, even clarification may inevitably entail some substantive choices.

<p>Data Act with amendments by Omnibus Proposal COM(2025) 837 final</p>	<p>Comments</p>	<p>ELI Proposal</p>
<p><i>Article 1</i> Subject matter and scope</p>		<p><i>Article 1</i> Subject matter and scope</p>
<p>1. This Regulation lays down harmonised rules, inter alia, on:</p> <ol style="list-style-type: none"> a. the making available of product data and related service data to the user of the connected product or related service; b. the making available of data by data holders to data recipients; c. the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there is an exceptional need for those data for the performance of a specific task carried out in the public interest; 	<p>This paragraph can be significantly simplified and streamlined, in particular as the list is not exhaustive anyway.</p>	<p>1. This Regulation lays down harmonised rules, inter alia, on:</p> <ol style="list-style-type: none"> a. the making available of data by data holders to other businesses or to consumers; b. the making available of data by data holders to public sector or Union bodies, where there is an exceptional need in the public interest; c. facilitating switching between data processing services; d. facilitating switching between data processing services;

<p>e. introducing safeguards against unlawful third-party access to non-personal data;</p> <p>ea. voluntary registration of data intermediation services;</p> <p>eb. voluntary registration of entities which collect and process data made available for altruistic purposes;</p> <p>ec. the establishment of a European Data Innovation Board;</p> <p>ed. data localisation requirements and the availability of data to competent authorities;</p> <p>ee. the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data; and</p> <p>f. the development of interoperability standards for data to be accessed, transferred and used.</p> <p>2. This Regulation covers personal and non-personal data, including the following types of data, in the following contexts:</p> <p>a. Chapter II applies to data, with the exception of content, concerning the performance, use and environment of connected products and related services;</p> <p>b. Chapter III applies to any private sector data that is subject to statutory data sharing obligations;</p> <p>c. Chapter IV applies to any private sector data accessed and used on the basis of contract between enterprises;</p> <p>d. Chapter V applies to any private sector data with a focus on non-personal data;</p> <p>e. Chapter VI applies to any data and services processed by providers of data processing services;</p> <p>f. Chapter VII applies to any non-personal data held in the Union by providers of data processing services.</p> <p>g. <i>Chapter VIIa applies to personal and non-personal data;</i></p>	<p>For the most part, this paragraph is not only superfluous, but also apt to mislead, due to overlap and friction with provisions on scope in the individual Chapters.</p> <p>The only important message it contains is that personal and non-personal data are covered, and this message can be combined with the message currently found in paragraph 5.</p>	<p>d. safeguards against unlawful third-country access to data;</p> <p>e. voluntary registration of data intermediation services and of entities which collect and process data made available for altruistic purposes;</p> <p>f. data localisation requirements within the Union;</p> <p>g. the re-use of certain data and documents held by public sector bodies or by certain public undertakings, and of research data;</p> <p>h. the development of interoperability standards for data to be accessed, transferred and used; and</p> <p>i. the establishment of a European Data Innovation Board.</p> <p>2. This Regulation covers personal and non-personal data, unless explicitly provided otherwise. This Regulation is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein.</p>
---	---	---

<p><i>h. Chapter VIIb applies to any non-personal data;</i></p> <p><i>i. Chapter VIIc applies to personal and non-personal data, namely the following:</i></p> <p><i>i. documents held by public sector bodies of Member States as referred</i></p> <p><i>(1) to in Article 32i(1), point (a) or by public undertakings as referred</i></p> <p><i>(2) to in Article 32i(1), point (b);</i></p> <p><i>ii. research data as referred to in Article 32i(1), point (c);</i></p> <p><i>iii. certain categories of protected data as referred to in Article 32i(1), point (a).</i></p>		
<p>3. This Regulation applies to:</p> <p>a. manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;</p> <p>b. users in the Union of connected products or related services as referred to in point (a);</p> <p>c. data holders, irrespective of their place of establishment, that make data available to data recipients in the Union;</p> <p>d. data recipients in the Union to whom data are made available;</p> <p>e. public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request;</p>	<p>Paragraph 3 on territorial scope suffers from several serious shortcomings, some of which put European businesses at a significant competitive disadvantage vis-à-vis businesses in third countries.</p>	<p>3. This Regulation applies to:</p> <p>a. manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;</p> <p>b. data holders within the meaning of Chapter II, irrespective of their place of establishment, of product data or related services data generated by connected products or related services as referred to in point (a);</p> <p>c. users in the Union of connected products or related services as referred to in point (a);</p> <p>d. data holders, irrespective of their place of establishment, that are obliged under other Union law to make data available to data recipients in the Union;</p> <p>e. data recipients to whom data are made available under this Regulation or other Union law;</p> <p>f. public sector bodies of Member States or Union bodies;</p>

<p>f. providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;</p> <p>g. participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.</p> <p>g. participants in data spaces.</p>	<p>Besides, provisions on the international scope with regard to the new provisions originating in the DGA, FFDR and ODD are lacking.</p>	<p>g. providers of data intermediation services and of entities which collect and process data made available for altruistic purposes, irrespective of their place of establishment, providing services to customers in the Union;</p> <p>h. providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;</p> <p>i. participants in data spaces established under Union law or Member State law in accordance with Union law.</p>
<p>4. Where this Regulation refers to connected products or related services, such references are also understood to include virtual assistants insofar as they interact with a connected product or related service.</p>	<p>This paragraph creates more confusion than clarity and can be deleted.</p>	
<p>5. This Regulation is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein, in particular Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive 2002/58/EC, including the powers and competences of supervisory authorities and the rights of data subjects. Insofar as users are data subjects, the rights laid down in Chapter II of this Regulation shall complement the rights of access by data subjects and rights to data portability under Articles 15 and 20 of Regulation (EU) 2016/679. In the event of a conflict between this Regulation and Union law on the protection of personal data or privacy, or national legislation adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data or privacy shall prevail.</p>	<p>This paragraph can be significantly shortened and simplified and merged with what is left of paragraph 2.</p>	

<p>6. This Regulation does not apply to or pre-empt voluntary arrangements for the exchange of data between private and public entities, in particular voluntary arrangements for data sharing.</p> <p>This Regulation does not affect Union or national legal acts providing for the sharing of, access to and the use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties, or for customs and taxation purposes, in particular Regulations (EU) 2021/784, (EU) 2022/2065 and (EU) 2023/1543 and Directive (EU) 2023/1544, or international cooperation in that area. This Regulation does not apply to the collection or sharing of, access to or the use of data under Regulation (EU) 2015/847 and Directive (EU) 2015/849. This Regulation does not apply to areas that fall outside the scope of Union law and in any event does not affect the competences of the Member States concerning public security, defence or national security, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and the maintenance of law and order. This Regulation does not affect the competences of the Member States concerning customs and tax administration or the health and safety of citizens.</p>	<p>This paragraph can be shortened and simplified.</p>	<p>4. This Regulation does not affect Union or national legal acts providing for the sharing of, access to and the use of data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the execution of criminal penalties, or for customs and taxation purposes, or international cooperation in that area.</p> <p>This Regulation does not apply to areas that fall outside the scope of Union law and in any event does not affect the competences of the Member States concerning public security, defence or national security, regardless of the type of entity entrusted by the Member States to carry out tasks in relation to those competences, or their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and the maintenance of law and order.</p>
<p>7. This Regulation complements the self-regulatory approach of Regulation (EU) 2018/1807 by adding generally applicable obligations on cloud-switching.</p>		
<p>8. This Regulation is without prejudice to Union and national legal acts providing for the protection of intellectual property rights, in particular Directives 2001/29/EC, 2004/48/EC and (EU) 2019/790.</p>	<p>This message is either superfluous or incorrect (cf. Chapter X) and can therefore be deleted.</p>	

<p>9. This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, and to protect their health, safety and economic interests, in particular Directives 93/13/EEC, 2005/29/EC and 2011/83/EU.</p>	<p>This paragraph can be shortened and simplified.</p>	<p>5. This Regulation complements and is without prejudice to Union law which aims to promote the interests of consumers and ensure a high level of consumer protection, including Directive 93/13/EEC.</p>
<p>10. This Regulation does not preclude the conclusion of voluntary lawful data sharing contracts, including contracts concluded on a reciprocal basis, which comply with the requirements laid down in this Regulation.</p>	<p>This message is superfluous and can, therefore, be deleted.</p>	
<p>11. Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public authorities and bodies governed by public law, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.</p> <p>12. Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.</p> <p>13. With regards to data and documents in scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation does not affect the possibility for Member States to adopt more detailed or stricter rules, provided that those rules allow for more extensive re-use of data and documents.</p>		<p>6. Chapter VIIb of this Regulation is without prejudice to laws, regulations, and administrative provisions that relate to the internal organisation of Member States and that allocate, among public sector bodies, powers and responsibilities for the processing of data without contractual remuneration of private parties, as well as to laws, regulations, and administrative provisions of Member States that provide for the implementation of such powers and responsibilities.</p> <p>7. Where sector-specific Union or national law requires public sector bodies, data intermediation services providers or recognised data altruism organisations to comply with specific additional technical, administrative or organisational requirements that relate to Chapters VIIa and VIIb, including through an authorisation or certification regime, those provisions of that sector-specific Union or national law shall also apply. Any such specific additional requirements shall be non-discriminatory, proportionate and objectively justified.</p> <p>8. With regards to data and documents in the scope of Section II of Chapter VIIc, Chapter VIIc of this Regulation does not affect the possibility for Member States to adopt more detailed or stricter rules, provided that those rules allow for more extensive re-use of data and documents.</p>

Article 2 Definitions		Article 2 Definitions
<p>13. 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use or make available data, including, where contractually agreed, product data or related service data, which it has retrieved or generated during the provision of a related service;</p>	<p>Given the objective to consolidate the Data Act, the DGA, FFDR and ODD into one single document, ELI finds it necessary to introduce a more general definition of 'data holder' in line with the DGA and ODD and inspired by the definition of 'controller' in Article 4 [7] GDPR to ensure coherence with Union law.</p> <p>For the purposes of Chapter II, a more specific definition tailored to connected products and related services is required, which should overcome the circularity and other flaws of the current definition.</p>	<p>13. 'data holder' with regard to certain data means a natural or legal person that, alone or jointly with others, determines the purposes and means of processing the data; it includes a controller within the meaning of Article 4, point (7), of Regulation (EU) 2016/679. For the purposes of Chapter II of this Regulation, it specifically means a natural or legal person other than the user of a connected product or related service that has, due to the design of the connected product or related service, direct access to the connected product or related service in a way enabling that person to retrieve product data or related services data without the help of the user.</p>
<p>Article 4 (8) <i>[analogous wording in Article 5 (11)]</i></p>		<p>Article 4 (8) <i>[analogous wording in Article 5 (11)]</i></p>
<p>In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, it is highly likely to suffer serious economic damage from the disclosure of trade secrets; despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. or that the disclosure of trade secrets to the user 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, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, in particular such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product; and It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.</p>	<p>The structure of the provision should be made more transparent and it should be clarified that the problem to be addressed in the first place is that the user (or data recipient) may not apply the technical or organisational measures agreed upon.</p>	<p>8. In exceptional circumstances, where the data holder is able to demonstrate that</p> <ol style="list-style-type: none"> a. the data holder or, where they are not the same person, the trade secret holder is highly likely to suffer serious economic damage if the user fails to apply the technical or organisational measures agreed upon; or b. the disclosure of trade secrets to the user 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, that data holder may refuse on a case-by-case basis a request for access to the specific data in question. <p>That demonstration shall be duly substantiated on the basis of objective elements, such as the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product. It shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.</p>

<p><i>Article 7</i> Scope of business-to-consumer and business-to-business data sharing obligations</p>	<p>Heading re-formulated in order to better reflect the content.</p>	<p><i>Article 7</i> Scope of obligations and restrictions under this Chapter</p>
<p>1. The obligations of this Chapter shall not apply to data generated through the use of connected products manufactured or designed or related services provided by a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service.</p> <p>The same shall apply to data generated through the use of connected products manufactured by or related services provided by an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.</p>	<p>Slightly re-phrased and re-formulated in the interest of transparency.</p>	<p>1. The obligations under Articles 3, 4 and 5 of this Chapter shall not apply to data generated through the use of connected products manufactured or designed or related services provided by</p> <ul style="list-style-type: none"> a. a microenterprise or a small enterprise, provided that that enterprise does not have a partner enterprise or a linked enterprise within the meaning of Article 3 of the Annex to Recommendation 2003/361/EC that does not qualify as a microenterprise or a small enterprise and where the microenterprise and small enterprise is not subcontracted to manufacture or design a connected product or to provide a related service; or b. an enterprise that has qualified as a medium-sized enterprise under Article 2 of the Annex to Recommendation 2003/361/EC for less than one year and to connected products for one year after the date on which they were placed on the market by a medium-sized enterprise.
	<p>Clarification added that the obligations of a seller, rentor or lessor do not apply to consumers.</p>	<p>2. The obligations under paragraphs 2 and 3 of Article 3 shall not apply to a seller, rentor or lessor who is a person acting in a private and non-commercial capacity.</p>
<p>2. Any contractual term which, to the detriment of the user, excludes the application of, derogates from or varies the effect of the user's rights under this Chapter shall not be binding on the user.</p>	<p>Integrated in Article 8 to remove friction and overlap.</p>	
<p><i>Article 8</i> Conditions under which data holders make data available to data recipients</p>		<p><i>Article 8</i> Conditions under which data holders make data available</p>

<p>1. Where, in business-to-business relations, a data holder is obliged to make data available to a data recipient under Article 5 or under other applicable Union law or national legislation adopted in accordance with Union law, it shall agree with a data recipient the arrangements for making the data available and shall do so under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner in accordance with this Chapter and Chapters II and IV.</p> <p>2. A contractual term concerning access to and the use of data, or liability and remedies for the breach or termination of data-related obligations, shall not be binding if it constitutes an unfair contractual term within the meaning of Article 13 or if, to the detriment of the user, it excludes the application of, derogates from or varies the effect of the user's rights under Chapter II.</p> <p>3. A data holder shall not discriminate regarding the arrangements for making data available between comparable categories of data recipients, including partner enterprises or linked enterprises of the data holder when making data available. Where a data recipient considers that the conditions under which data has been made available to it are discriminatory, the data holder shall without undue delay provide the data recipient, upon its reasoned request, with information showing that there has been no discrimination.</p>	<p>Paragraph 1 has been merged with Article 12 on scope, and errors in the description of the scope have been corrected.</p> <p>The provision on FRAND has been moved to paragraph 2.</p> <p>Paragraph 2 was misleading and arguably incorrect, at least if what is written in Recital 25 and the Commission Recommendation on model contractual terms is correct.</p>	<p>1. This Chapter shall apply where, in business-to-business relations, a data holder is obliged under Articles 4 or 5 or under applicable Union law or national legislation adopted in accordance with Union law, to make data available to a user or a data recipient.</p> <p>2. Where, in business-to-business relations, a data holder is obliged to make data available to a data recipient under Article 5 or under other applicable Union law or national legislation adopted in accordance with Union law, it shall agree with a data recipient the arrangements for making the data available and shall do so under fair, reasonable and non-discriminatory terms and conditions and in a transparent manner in accordance with this Chapter and Chapters II and IV.</p> <p>3. The contract shall not derogate, to the detriment of the user or the data recipient, from the rights and obligations under Chapter II and this Chapter or under relevant Union law or national legislation adopted in accordance with Union law in any material way, and such material derogation shall not be binding on the user or data recipient.</p> <p>Where the data holder and the user or data recipient agree to modify or restrict certain rights or obligations, in particular the user's right to disclose data it has received under Article 4 to a third party, such modification or restriction shall not be considered to be material where it is not to the detriment of the user or data recipient, taking into account any adequate compensation.</p>
<p>4. A data holder shall not make data available to a data recipient, including on an exclusive basis, unless requested to do so by the user under Chapter II.</p>	<p>The meaning of this provision remains entirely in the obscure – the way it is drafted is obviously incorrect.</p>	
<p>5. Data holders and data recipients shall not be required to provide any information beyond what is necessary to verify compliance with the contractual terms agreed for making data available or with their obligations under this Regulation or other applicable Union law or national legislation adopted in accordance with Union law.</p>	<p>This is far too broad and arguably largely incorrect – additional information obligations may follow from a number of different laws, including general contract law and the law of tort. Also, there may be joint controllership under the GDPR, which entails all sorts of duties to cooperate.</p>	

<p>6. Unless otherwise provided for in Union law, including Article 4(6) and Article 5(9) of this Regulation, or by national legislation adopted in accordance with Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets.</p>		<p>4. Unless otherwise provided for in Union law, including Article 4(6) and Article 5(9) of this Regulation, or by national legislation adopted in accordance with Union law, an obligation to make data available to a data recipient shall not oblige the disclosure of trade secrets.</p>
<p><i>Article 11</i> Technical protection measures on the unauthorised use or disclosure of data</p>	<p>The heading of current Article 11 is incorrect. Only the first paragraph concerns technical safeguards, while the remainder covers remedies for infringements. This provision should be split into two different Articles.</p>	<p><i>Article 11</i> Technical protection measures</p>
<p>1. A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with Articles 4, 5, 6, 8 and 9, as well as with the agreed contractual terms for making data available. Such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5 or any right of a third party under Union law or national legislation adopted in accordance with Union law. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.</p>	<p>Split into three paragraphs to enhance transparency.</p>	<p>1. A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with this Regulation as well as with the agreed contractual terms for making data available.</p> <p>2. Technical protection measures shall not be used to circumvent obligations following from this Regulation or other Union law or national legislation adopted in accordance with Union law, such as by discriminating between data recipients or hindering a user or third party from exercising their rights.</p> <p>3. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.</p>
	<p>The new Article 11a needs an appropriate heading</p>	<p><i>Article 11a</i> Remedies in the case of infringements</p>

<p>2. In the circumstances referred to in paragraph 3, the third party or data recipient shall comply, without undue delay, with the requests of the data holder and, where applicable and where they are not the same person, the trade secret holder or the user:</p> <ul style="list-style-type: none"> a. to erase the data made available by the data holder and any copies thereof; b. to end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where there is a serious risk that the unlawful use of those data will cause significant harm to the data holder, the trade secret holder or the user or where such a measure would not be disproportionate in light of the interests of the data holder, the trade secret holder or the user; c. to inform the user of the unauthorised use or disclosure of the data and of the measures taken to put an end to the unauthorised use or disclosure of the data; d. to compensate the party suffering from the misuse or disclosure of such unlawfully accessed or used data. <p>3. Paragraph 2 shall apply where a third party or a data recipient has:</p> <ul style="list-style-type: none"> a. for the purposes of obtaining data, provided false information to a data holder, deployed deceptive or coercive means or abused gaps in the technical infrastructure of the data holder designed to protect the data; b. used the data made available for unauthorised purposes, including the development of a competing connected product within the meaning of Article 6(2), point (e); 	<p>Content of Article 11(2) moved to Article 11a(2), and content of Article 11(3) moved to Article 11a(1).</p>	<p>1. The data holder and, where applicable and where they are not the same person, the trade secret holder, shall have the remedies listed in paragraph 2 where a data recipient, a user or any third party that has received data from a data recipient or a user has committed any of the following infringements:</p> <ul style="list-style-type: none"> a. for the purposes of obtaining data, provided false information, deployed deceptive or coercive means or abused gaps in technical infrastructure designed to protect the data; b. used the data made available for unauthorised purposes, including the development of a competing connected product within the meaning of Article 6(2), point (e); c. unlawfully disclosed data to another party; d. not maintained the technical and organisational measures agreed pursuant to Articles 4(6) or 5(9); or e. altered or removed technical protection measures applied by the data holder pursuant to Article 11 without the agreement of the data holder. <p>The user shall have the same remedies where the data recipient or any third party that has received data from a data recipient infringes Article 6(2), point (a) or (b).</p> <p>2. The infringing party shall comply, without undue delay, with the requests of the data holder and, where applicable and where they are not the same person, the trade secret holder or the user:</p> <ul style="list-style-type: none"> a. to erase the data made available by the data holder and any copies thereof; b. to end the production, offering or placing on the market or use of goods, derivative data or services produced on the basis of knowledge obtained through such data, or the importation, export or storage of infringing goods for those purposes, and destroy any infringing goods, where
--	--	---

<p>c. unlawfully disclosed data to another party;</p> <p>d. not maintained the technical and organisational measures agreed pursuant to Article 5(9); or</p> <p>e. altered or removed technical protection measures applied by the data holder pursuant to paragraph 1 of this Article without the agreement of the data holder.</p> <p>4. Paragraph 2 shall also apply where a user alters or removes technical protection measures applied by the data holder or does not maintain the technical and organisational measures taken by the user in agreement with the data holder or, where they are not the same person, the trade secrets holder, in order to preserve trade secrets, as well as in respect of any other party that receives the data from the user by means of an infringement of this Regulation.</p>		<p>i. there is a serious risk that the unlawful use of those data will cause significant harm to the data holder, the trade secret holder or the user; and</p> <p>ii. such a measure would not be disproportionate in light of the interests of the data holder, the trade secret holder or the user;</p> <p>c. to inform the user of the unauthorised use or disclosure of the data and of the measures taken to put an end to the unauthorised use or disclosure of the data;</p> <p>d. to compensate the party suffering from the misuse or disclosure of such unlawfully accessed or used data.</p>
	<p>Clarification added that other remedies remain unaffected.</p>	<p>3. The remedies listed in paragraph 2 are without prejudice to remedies that follow from other Union law or national legislation adopted in accordance with Union law, including contract law, tort law and unfair competition law, or from contractual provisions agreed in accordance with this Chapter and Chapters II and IV.</p>
<p>5. Where the data recipient infringes Article 6(2), point (a) or (b), users shall have the same rights as data holders under paragraph 2 of this Article.</p>	<p>Included in Article 11a(1).</p>	
<p><i>Article 12</i> Scope of obligations for data holders obliged pursuant to Union law to make data available</p>		
<p>1. This Chapter shall apply where, in business-to-business relations, a data holder is obliged under Article 5 or under applicable Union law or national legislation adopted in accordance with Union law, to make data available to a data recipient.</p>	<p>Paragraph (1) merged with Article 8(2). Paragraph (2) merged with Article 8(3).</p>	

<p>2. A contractual term in a data sharing agreement which, to the detriment of one party, or, where applicable, to the detriment of the user, excludes the application of this Chapter, derogates from it, or varies its effect, shall not be binding on that party.</p>		
<p><i>Article 25</i> Contractual terms concerning switching</p>	<p>Current Article 25 conflates the requirement to have a written contract with the customer’s switching rights, which creates uncertainty about the consequences of non-compliance. ELI proposes splitting this article into two.</p>	<p><i>Article 25</i> Contractual terms concerning switching</p>
<p>1. The rights of the customer and the obligations of the provider of data processing services in relation to switching between providers of such services or, where applicable, to an on-premises ICT infrastructure shall be clearly set out in a written contract. The provider of data processing services shall make that contract available to the customer prior to signing the contract in a way that allows the customer to store and reproduce the contract.</p>		<p>1. The rights of the customer and the obligations of the provider of data processing services in relation to switching between providers of such services or, where applicable, to an on-premises ICT infrastructure shall be clearly set out in a written contract. The provider of data processing services shall make that contract available to the customer prior to signing the contract in a way that allows the customer to store and reproduce the contract.</p>
	<p>Such a provision was clearly lacking in Chapter VI.</p>	<p>2. The contract shall not derogate, to the detriment of the customer, from the rights and obligations under this Chapter in any material way, and such material derogation shall not be binding on the customer.</p>
		<p><i>Article 25a</i> Customer rights concerning switching</p>
<p>2. Without prejudice to Directive (EU) 2019/770, the contract referred to in paragraph 1 of this Article shall include at least the following:</p> <p>a. clauses allowing the customer, upon request, to switch to a data processing service offered by a different provider of data processing services or to port all exportable data and digital assets to an on-premises ICT infrastructure, without undue delay and in any event not after the mandatory maximum transitional period of 30 calendar days, to be initiated after the maximum notice period referred to in point (d), during which the service contract remains applicable and during which the provider of data processing services shall:</p>	<p>The remaining paragraphs of Article 25 should be phrased as statutory duties.</p> <p>Provisions should be rearranged and significantly simplified and presented in a more transparent manner.</p>	<p>1. The customer has a right, at any time, to request the provider of data processing services to do any of the following, subject to any necessary cooperation on the part of the customer or the provider indicated by the customer:</p> <p>a. port the customer’s data to a different provider of data processing services indicated by the customer;</p> <p>b. port the customer’s data to on-premises ICT infrastructure of the customer;</p> <p>c. erase the customer’s data.</p>

<ul style="list-style-type: none"> i. provide reasonable assistance to the customer and third parties authorised by the customer in the switching process; ii. act with due care to maintain business continuity, and continue the provision of the functions or services under the contract; iii. provide clear information concerning known risks to continuity in the provision of the functions or services on the part of the source provider of data processing services; iv. ensure that a high level of security is maintained throughout the switching process, in particular the security of the data during their transfer and the continued security of the data during the retrieval period specified in point (g), in accordance with applicable Union or national law; <p>b. an obligation of the provider of data processing services to support the customer's exit strategy relevant to the contracted services, including by providing all relevant information;</p> <p>c. a clause specifying that the contract shall be considered to be terminated and the customer shall be notified of the termination, in one of the following cases:</p> <ul style="list-style-type: none"> i. where applicable, upon the successful completion of the switching process; ii. at the end of the maximum notice period referred to in paragraph (d), where the customer does not wish to switch but to erase its exportable data and digital assets upon service termination; <p>d. a maximum notice period for initiation of the switching process, which shall not exceed two months;</p>		<p>2. The provider of data processing services must take action in accordance with the customer's request without undue delay. A switching and porting process must, in any event, be completed within a maximum transitional period not exceeding 30 calendar days after receiving the customer's request and, where relevant, expiry of any notice period that has been contractually agreed and that must not exceed two months.</p> <p>Where the mandatory maximum transitional period as provided for in subparagraph 1 is technically unfeasible, the provider shall notify the customer within 14 working days of receipt of the customer's request and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven months.</p> <p>The customer has the right to extend the transitional period once for a period that the customer considers more appropriate for its own purposes.</p> <p>3. During the transitional period, the provider of data processing services shall:</p> <ul style="list-style-type: none"> a. provide reasonable assistance to the customer and third parties authorised by the customer in the switching process; b. act with due care to maintain business continuity, and continue the provision of the functions or services under the contract; c. support the customer's exit strategy relevant to the contracted services, such as by providing all relevant information, including information concerning known risks to continuity in the provision of the services on the source provider's own part; d. ensure that a high level of security is maintained throughout the switching process and during data transfer, insofar as security falls within the source provider's control, and ensure the continued security of the data for the duration of the retrieval period specified in paragraph 4.
--	--	--

<p>e. an exhaustive specification of all categories of data and digital assets that can be ported during the switching process, including, at a minimum, all exportable data;</p> <p>f. an exhaustive specification of categories of data specific to the internal functioning of the provider's data processing service that are to be exempted from the exportable data under point l of this paragraph where a risk of breach of trade secrets of the provider exists, provided that such exemptions do not impede or delay the switching process provided for in Article 23;</p> <p>g. a minimum period for data retrieval of at least 30 calendar days, starting after the termination of the transitional period that was agreed between the customer and the provider of data processing services, in accordance with point (a) of this paragraph and paragraph 4;</p> <p>h. a clause guaranteeing full erasure of all exportable data and digital assets generated directly by the customer, or relating to the customer directly, after the expiry of the retrieval period referred to in point g. or after the expiry of an alternative agreed period at a date later than the date of expiry of the retrieval period referred to in point g., provided that the switching process has been completed successfully;</p> <p>i. switching charges, that may be imposed by providers of data processing services in accordance with Article 29.</p> <p>3. The contract referred to in paragraph 1 shall include clauses providing that the customer may notify the provider of data processing services of its decision to perform one or more of the following actions upon termination of the maximum notice period referred to in paragraph 2, point d.:</p> <p>a. switch to a different provider of data processing services, in which case the customer shall provide the necessary details of that provider;</p>		<p>4. The customer may request the contract to be terminated with effect from the successful completion of a switching and porting process or at any specific date thereafter, without prejudice to any other termination rights following from the contract or applicable law. From termination taking effect, the customer no longer has to pay the remuneration agreed, subject to any charges that have been contractually agreed and are consistent with Article 29. The customer may restrict termination to a separable part of the services where this is technically possible and agreed in the contract or allowed by applicable law.</p> <p>In the event of termination, the provider of data processing services shall:</p> <p>a. grant the customer an additional period for data retrieval of at least 30 calendar days from termination taking effect, unless the customer explicitly requests immediate erasure; and</p> <p>b. guarantee full erasure of the customer's data, or the relevant part of the customer's data, after the expiry of the retrieval period referred to in point (a).</p> <p>Point b. of the previous subparagraph does not prevent the data processing service provider from continuing to store the customer's data to the extent required by law or as far as is strictly necessary for the provider's or a third party's legitimate interests, such as the pursuit or defence of legal claims, unless those interests are overridden by the customer's legitimate interests to have the data erased.</p>
---	--	--

<p>b. switch to an on-premises ICT infrastructure;</p> <p>c. erase its exportable data and digital assets.</p> <p>4. Where the mandatory maximum transitional period as provided for in paragraph 2, point (a) is technically unfeasible, the provider of data processing services shall notify the customer within 14 working days of the making of the switching request, and shall duly justify the technical unfeasibility and indicate an alternative transitional period, which shall not exceed seven months. In accordance with paragraph 1, service continuity shall be ensured throughout the alternative transitional period.</p> <p>5. Without prejudice to paragraph 4, the contract referred to in paragraph 1 shall include clauses providing the customer with the right to extend the transitional period once for a period that the customer considers more appropriate for its own purposes.</p>		
<p><i>Article 29</i> Gradual withdrawal of switching charges</p>	<p>Heading slightly re-phrased</p>	<p><i>Article 29</i> Charges in connection with switching and termination</p>
<p>1. From 12 January 2027, providers of data processing services shall not impose any switching charges on the customer for the switching process.</p> <p>2. From 11 January 2024 to 12 January 2027, providers of data processing services may impose reduced switching charges on the customer for the switching process.</p> <p>3. The reduced switching charges referred to in paragraph 2 shall not exceed the costs incurred by the provider of data processing services that are directly linked to the switching process concerned.</p>	<p>Article 29 as proposed by ELI would not include transitional provisions (which should be in Article 50).</p> <p>However, it would include the important qualifications stated in Recital 89 and provide guidance on the conditions for early termination penalties.</p>	<p>1. Providers of data processing services shall not impose any charges on the customer for the switching process.</p> <p>However, providers may charge customers with costs incurred that are directly linked to the switching process concerned as far as such costs exceed the costs which the provider could reasonably anticipate when concluding the contract because they are due to shortcomings in the sphere of the customer or the destination provider indicated by the customer, including failure to cooperate, lack of expertise or deficiencies in the ICT infrastructure.</p> <p>2. As far as compatible with other Union or Member State law, the contract may provide for a degressive calculation of standard service fees or any other benefit, such as loyalty rewards, which customers become entitled to after a certain contract period.</p>

		<p>3. The contract may provide for fair and reasonable early termination penalties where the contract is for a fixed duration and the customer terminates the contract before the expiry of that duration. Such penalties must</p> <ul style="list-style-type: none"> a. not exceed the payments which would have become due at a minimum until the end of the contract period; and b. adequately reflect any reduction, due to the early termination, in effort and expenses on the part of the provider.
<p>4. Before entering into a contract with a customer, providers of data processing services shall provide the prospective customer with clear information on the standard service fees and early termination penalties that might be imposed, as well as on the reduced switching charges that might be imposed during the timeframe referred to in paragraph 2.</p> <p>5. Where relevant, providers of data processing services shall provide information to a customer on data processing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.</p>		<p>4. Before entering into a contract with a customer, providers of data processing services shall provide the prospective customer with clear information on the standard service fees and early termination penalties that might be imposed.</p> <p>Where relevant, providers of data processing services shall provide information to a customer on data processing services that involve highly complex or costly switching or for which it is impossible to switch without significant interference in the data, digital assets or service architecture.</p>
<p>6. Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way.</p>		<p>5. Where applicable, providers of data processing services shall make the information referred to in paragraphs 4 and 5 publicly available to customers via a dedicated section of their website or in any other easily accessible way.</p>
<p>7. The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by establishing a monitoring mechanism for the Commission to monitor switching charges, imposed by providers of data processing services on the market to ensure that the withdrawal and reduction of switching charges, pursuant to paragraphs 1 and 2 of this Article are to be attained in accordance with the deadlines laid down in those paragraphs.</p>	<p>Shortened and streamlined.</p>	<p>6. The Commission is empowered to adopt delegated acts in accordance with Article 45 to supplement this Regulation by establishing a monitoring mechanism for the Commission to monitor the implementation of this Article.</p>

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.



ELI

EUROPEAN
LAW
INSTITUTE