EUROPEAN
COMMISSION

Brussels, XXX
[…](2026) XXX draft

COMMUNICATION FROM THE COMMISSION

Guidelines on the calculation of reasonable compensation as set out in Article 9 of Regulation (EU) 2023/2854 (Data Act)

COMMUNICATION FROM THE COMMISSION

Guidelines on the calculation of reasonable compensation as set out in Article 9 of Regulation (EU) 2023/2854 (Data Act)

1. INTRODUCTION

1. [The Commission adopted these guidelines on the calculation of reasonable compensation (hereinafter the 'Guidelines') in accordance with Article 9(5) of Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), after receiving advice from the European Data Innovation Board in accordance with Article 9(5) and 42 of the Data Act. The Commission held an industry webinar attended by around 300-350 participants on 15 July 2025.]

2. The primary aim of the Data Act is to strengthen the European data economy by removing barriers to data sharing, while preserving the incentives for those who invest in data technologies.

3. These Guidelines intend to provide data holders and data recipients with practical guidance on how to calculate reasonable compensation in the context of an obligation to make data available pursuant to Union law or national legislation adopted in accordance with Union law. The data holder's right to request reasonable compensation from data recipients is essential to ensuring a fair distribution of benefits generated in the data value chain.

4. Chapter III of the Data Act, which includes Article 9 on reasonable compensation for making data available, establishes rules governing mandatory business-to-business data-sharing that are applicable across all sectors of the Union economy. These Guidelines are meant to be used in all relevant situations, in particular those covered by Chapter II of the Data Act (more specifically business data sharing in the context of the Internet-of-Things). As regards data sharing obligations established by legislation other than under the Data Act, Chapter III applies only in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which have entered into force after 12 September 2025, in line with Article 50, insofar as these obligations are not subject to a specific compensation regime.

5. These Guidelines leave room for the development of sector-specific mechanisms where and to the extent foreseen in applicable EU law according to Art 9 (6) of the Data Act.

6. The binding interpretation of EU legislation is the exclusive competence of the Court of Justice of the European Union. Therefore, the Commission's interpretation of the Data Act as regards the calculation of reasonable compensation does not have any bearing on the interpretation which may be given by the Court of Justice of the European Union.

2. FRAND PRINCIPLES

7. Chapter III of the Data Act establishes the general framework for mandatory business-to-business (B2B) data sharing. According to Article 8, the data holder and data recipient must agree on the arrangements for making data available in accordance with "fair, reasonable and non-discriminatory terms and conditions" ('FRAND') and "in a transparent manner". Article 9 specifies rules for the compensation that can be requested by data holders for making data available.

8. The concept of FRAND originates from the licensing of standard-essential patents (SEPs). However, only very limited inspiration can be drawn from that for the purpose of these Guidelines. Sharing data to comply with a regulatory obligation is different from sharing a SEP in the context of SEP licensing. In the SEP context, there is no need for technical cooperation between the patent holder and the party requiring a licence as the information required (the patent) is publicly known. As a result, it is typically the patent holder that will start proceedings against a party that uses the SEP without a licence. Under the Data Act, the situation would typically be the opposite on both counts. First, the data holder, who technically holds control over data access, is legally obliged to cooperate with the data recipient to conclude a contract for data sharing. Second, as a result of the need of the data holder to cooperate, data recipients would need to start proceedings if a data holder applies a hold out or hold up strategy. Considering these structural advantages of the data holder, the case law on SEP situations cannot be automatically extrapolated to the interpretation of the FRAND criteria under the Data Act.

3. GENERAL COMPENSATION REGIME

9. Article 9 differentiates between micro, small, and medium-sized enterprises (SMEs), as defined by Article 2 of the Annex to Commission Recommendation 2003/361/EC[1], or not-for-profit research organisations and other data recipients. In particular, Article 9(4) provides that any compensation charges to SMEs and not-for-profit research organisations must not exceed the costs incurred in making the data available (c.f. section 4.4. of these Guidelines).

10. Article 9(1) specifies that "any compensation agreed upon" shall be "non-discriminatory and reasonable and may include a margin". Article 9(3) establishes that the compensation may also depend on the volume, format, and nature of the data.

11. This means, firstly, that compensation is not mandatory. Data holders may choose to make the data available for free, be it for commercial purposes, public interest objectives, or any other reason. Also, compensation "*may"* include a margin (i.e. an additional amount added to the base costs incurred by the data holder which represents a profit or a fair return for their efforts, risks, or investments). A margin is therefore not mandatory.

[1] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, Official Journal L 124, 20/05/2003 P. 0036 - 0041

12. The interpretation of the "non-discriminatory" element can build on a body of non-discrimination legislation and case-law, which reflects the principle of equal treatment, except if justified by objective reasons. The difficult element is to consider which entities are in comparable categories for them to have a right to receive equal treatment. Certain distinctions are easier to make, such as whether an entity is for profit or not-for-profit.

13. Differentiating between data recipients is not justified where access is refused or penalised simply because a recipient is a current or potential competitor (e.g. in the product market or in services), where criteria are applied selectively or opaquely, or where a vague justification (e.g. "public interest") is invoked. In addition, if a data holder (e.g. the manufacturer of a connected product) has a statutory (i.e. linked enterprises) or contractual relationship with a data recipient for the provision of a related service for which the data may be used (for instance, 'affiliated/partner' repairers for the repair of a car or aeroplane manufactured by the data holder), the data holder should not discriminate between its affiliated/partner and that partner's competitors.

14. By contrast, differentiation can be justified when it is tied to objective requirements. Such objective requirements include, for instance, additional costs that

    - are necessary to meet security, compliance or confidentiality standards,
    - stem from measures to protect or maintain the confidentiality of data of a sensitive nature , including safety-critical data, personal data, or trade secrets, or
    - reflect objective technical burdens related to, for instance, the data format, volume or frequency, real-time versus delayed access, or the effort to prepare certain datasets.

15. Any distinction should be proportionate and aimed at achieving legitimate interests such as protecting innovation and trade secrets and maintaining a level-playing field.

16. The "reasonable" element seeks to ensure that the amount of the compensation should not be economically prohibitive and deter potential data recipients from accessing and using data. It evaluated on a case-by-case assessment of the specific terms and conditions that underpin the agreement between the data holder and data recipient.

17. Unless otherwise provided by law, data holders should have room to design bundles of data and calculate the compensation accordingly, rather than a strict obligation to provide mechanisms allowing for data recipients to pick and choose any possible combination of data points. In this context, data bundling refers to the practice by which a data holder groups or aggregates multiple data items or datasets together and makes them available as a single package to a data recipient. Such bundles prevents data holders from incurring unnecessarily high upfront implementation costs for itemised contracting per data point. The bundle design needs to reflect actual or reasonably expected demand (e.g. based on common sector specific use-cases such as fleet management services in the automotive sector), and serve the lawful, intended use by the data recipient. A data holder may not condition access to a specific dataset on the acceptance of additional datasets the data recipient did not request or need. The design

should not be structured in a way that distorts or discourages data recipients' choices. It should not make the exercise of the data access right difficult in practice.

18. Undertakings holding a dominant position should in their bundling policy comply with Article 102 of the Treaty on the Functioning of the European Union ('TFEU'). Within the limits set by Union or national law and the applicable contract, data recipients should not be required to compensate for data beyond what is needed to provide their services or meet their needs.

19. For data within scope of Chapter II Data Act, any such bundling practice must be part of the pre-contractual information under Article 3(2) and (3), for instance through a dedicated webpage, in the user manual, or on the product packaging (Recital 24). There may be sector specific guidance[2].

4. DETERMINING THE COMPENSATION

20. It is important to establish what are "costs incurred in making the data available" (Article 9(2)(a) of the Data Act, see section 4.1), since only these costs can be included in the calculation of the compensation to be paid by SMEs and not-for-profit research organisations (see section 4.4).

21. Besides "costs" under Article 9(2)(a), the Data Act also establishes the "investment" category under Article 9(2)(b) (see section 4.2). Costs under Article 9(2)(a) refer to costs directly linked to an individual request and necessary to making data available (c.f. Recital 47 and 49). Investments under Article 9(2)(b) relate to investments that allow for data collection and production in the first place.

22. Data holders should carefully assess and categorize expenditures when calculating compensation. Clear delineation avoids the risk of double charging, where the same expenditure is claimed twice (from users or data recipients), or misallocation of expenditure.

4.1. Indicative elements for the calculation of compensation under Article 9(2)(a)

4.1.1. Cost of preparing and formatting the dataset

23. *Formatting the data*: Article 5(1) of the Data Act requires data holders to make data available, inter alia, in a "structured, commonly used and machine-readable format". This means that where a data holder stores data in an uncommon or proprietary format, and where a structured, commonly used and machine-readable format exists, the costs of reformatting to ensure compliance with a request under Article 5(1) cannot be included in the calculation of the compensation. Where the data recipient requires another specific format other than what would satisfy the abovementioned obligation, the costs of such reformatting can be included in the calculation of the compensation.

24. *Selecting a sub-set of data*: Where the request pertains to a specific subset of data which cannot be automatically extracted via an Application Programming Interface

[2] See, for example. paragraph 67 of the Commission notice — Supplementary guidelines on vertical restraints in agreements for the sale and repair of motor vehicles and for the distribution of spare parts for motor vehicles paragraph, OJ C 138, 28.5.2010, pp. 16–27

(API), the data holder can include the cost of making this selection in the calculation of the compensation.

25. *Transforming the data to protect data subjects*: This is relevant when the requesting data recipient acts on behalf of a user who is not the data subject for the data in question and could e.g. include the cost of anonymisation or any other technique that is designed to protect data subjects pursuant to Union or national law on the protection of personal data (c.f. Recital 7 and Article 5(13) Data Act). This can be included in the calculation of the compensation, but only when such costs are attributable to the specific request.

26. *Protecting commercially confidential data (trade secrets)*: Pursuant to Article 5(9) of the Data Act, data holders should clearly identify data protected as trade secrets (for example, in the metadata) and agree with the data recipient on proportionate technical and organisational measures to safeguard their confidentiality and preserve their nature as trade secrets. Data qualifies as a trade secret where it meets the definition under the Trade Secrets Directive, namely that it is secret, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret. Therefore, a data holder may not recover costs arising solely from measures undertaken on their side to identify and protect trade secrets. Costs incurred on the data recipient's side are to be borne by the data recipient. The compensation to be agreed between the parties should relate only to the measures necessary to maintain confidentiality when the data identified as trade secrets is lawfully disclosed, in particular to ensuring that it retains its nature as a trade secret once shared.

27. With respect to the preceding paragraph on protecting commercially confidential data (trade secrets), incremental costs arising specifically from a data recipient's access to the trade secret data are legitimate to recover. The intention is to distinguish between the data holder's baseline obligations and the additional measures triggered by the Data Act's obligation to disclose trade secrets. Legitimate recoverable costs by the data holder include negotiating a contract, liability arrangement, or non-disclosure agreement tailored to a request including trade secrets, audits of the data recipient's compliance with the protective measures, setting up recipient-specific technical measures (e.g. access controls, encryption), or using a neutral trusted third party or intermediary to handle the trade secret encumbered data. This ensures that only disclosure-related expenses are included in the compensation and avoids double-charging for protections the data holder already had in place. The objective is to safeguard the confidentiality of trade secrets without creating disproportionate barriers to access. While the data holder determines the measures necessary to protect the trade secret, they must strictly apply the principle of necessity as described in section 4.2.

28. As announced upon the entry into application of the Data Act, the Commission will adopt guidance on the protection of trade secrets under the Data Act. This guidance will complement these Guidelines by clarifying in particular the circumstances under which the trade secrets "handbrake" applies.

4.1.2. Cost of dissemination

29. *Dissemination:* This refers to costs incurred in the process of electronically distributing or transmitting data to the data recipient. It includes, for instance, costs for operating

the licensing or access tools that enable data sharing, such as a web portal or an API which is secure enough to prevent unauthorised access, as well as staff costs related to processing the data access request.

30. *Verifying the qualification of a person as a data recipient:* This relates to the onboarding costs (creation of a new account for the data recipient, verification of its identity as well as of persons authorized to make requests), and costs for verifying whether a company is an SME[3] or not-for-profit research organisation. It is possible that the EU Digital Identity Wallet[4] and the 'European Business Wallet', if adopted, will bring down these costs.

4.1.3. Cost of storage

31. *Data storage*: The data holder may choose to store the data in a dedicated IT environment (on premise or cloud solution) for the purpose of making it available to user and data recipients, independent of the IT environment that the data holder uses for its own purposes. In such case, storage costs linked to making data available to data recipients may be included in the calculation of the compensation. Storage costs not linked to making data available to users, on the other hand, should not be included in the calculation of the compensation. If the data holder stores the data in an environment that they also use for their own purpose, storage costs should only be part of the cost calculation to the extent that the environment is used for storing data with a view to make it available to data recipients. If there is no additional cost of data storage, there is no reason to charge data recipients for such costs.

4.2. 'Necessity' of the cost items under Article 9(2)(a)

32. Data holders should only add cost items that are necessary. Only costs that clearly result from a specific request and are required to fulfil the purpose of making the data available may be charged. Data holders should define cost categories in a comparable and auditable manner. Generally, costs need to be:

    i. incremental (that is, relating to the extra costs on top of normal business activities that arise due to a request)
    ii. objective
    iii. measurable, and
    iv. proportionate to the purpose of making the data available.

33. It is important that data holders define and apply cost categories, in particular incremental costs, in a comparable and auditable manner. Without such practical safeguards, data recipients, and in particular SMEs, may face significant difficulties in assessing and challenging compensation requests where data holders attempt to

[3] SMEs are encouraged to submit a self-declaration using the Commission's "Model declaration on the information relating to the qualification of an enterprise as an SME"

[4] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

broaden the interpretation of incremental costs, for example by relying on manual or inefficient processes.

34. It would be illegitimate for data holders to pass on overhead, sunk costs, speculative risks or ordinary business expenses as access-related charges, as this would undermine the FRAND principles. Other examples of unnecessary costs would be broad data cleaning, enhancement, or quality initiatives not necessary for a specific request. Warranties for the quality of the data should only be included if they were requested by the data recipient and in any event only if objectively necessary (the data collection and dissemination method may be of sufficient quality to make additional legal warranties unnecessary).

35. Data holders do not have to necessarily use the solution that comprises the minimum costs. They can rely on the reasonably available options. While smart contracts bring down the costs of contracting, not all companies are able nor ready to use them. Also, well-functioning dissemination mechanisms may already be in place (e.g. a web portal), so investments in an alternative and easier-to-use means (e.g. an API) may only be justified once upfront investment costs have been amortised. Similarly, API design may allow data recipients to select only a subset of data, but such design may not fit all data recipients' needs. For certain data recipients, manual processes may be necessary, triggering higher costs. Data holders should make reasonable assessments on what costs are necessary and what improvements in the cost structure can be made to keep costs reasonable.

36. In most cases, costs under Article 9(2)(a) will represent one-off costs that are triggered once for each data recipient (e.g. onboarding, initial contract negotiation, implementation of security settings), or in limited cases, once per request (e.g. defining the scope of the request, preparing and delivering a specific dataset). Where a data recipient seeks to receive data regularly or continuously, e.g. on a subscription basis, these costs should be spread over the duration of the subscription[5] (c.f. section 5 of these Guidelines).

4.3. Calculating investments and margin

37. As specified in Article 9(1) and Recital 47, a reasonable compensation may include a margin. When calculating the margin, the investments in the collection or production of data shall be taken into account; Section 4.3.2. of the Guidelines explores boundaries for such calculation. As explained in Recital 46, this principle shall "promote" continued "investment in generating and making available valuable data".

4.3.1. Indicative investment elements for the calculation of compensation under Article 9(2)(b)

38. *Collection of already existing data*: Investments to obtain, source, intake, or seek out data that already exists. This includes, for example, moving data from the original

[5] Cf. Section 4.1.1.3. of European Commission: Directorate-General for Justice and Consumers, Monti, G., Tombal, T. and Graef, I., *Study for developing criteria for assessing "reasonable compensation" in the case of statutory data access right – Study for the European Commission Directorate-General Justice and Consumers – Final report*, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2838/19186.

source into the data holder's environment (e.g. telecommunication costs); developing and deploying the IT systems necessary to receive and organise it (e.g. database, data warehouse, data lakes); the equipment or services that host it (e.g. servers acquired by the data holder, plus relevant operational costs such as electricity, security, and maintenance); tools that automate data collection (e.g. web scrapers). This does not include creating new data or the steps necessary to curate, prepare and make the data available to others.

39. *Production or generation of new data*: Investments whose primary purpose is to create original datasets, rather than source what already exists. This covers investments to deploy and operate physical instruments (e.g. sensors, meters, cameras) as well as virtual data generating technologies (e.g. web forms, surveys, simulations, digital twins). Where the data did not previously exist, it can also include investments in infrastructure or environments to create or capture it (e.g. new sensors, data storage units, or edge computing). This does not imply any obligation to retrofit connected products or create new data (c.f. definition of 'readily available data' in Article 2(17)). Activities aimed at preparing or delivering data to other parties (e.g. cleaning, anonymising, APIs, access controls) are outside this category.

4.3.2. Assessing the extent to which investments under Article 9(2)(b) should be taken into account when calculating the margin

40. It follows from the wording "shall take into account in particular" in Article 9(2) that several factors can play a role in the calculation of compensation and therefore of the margin. Any margin should according to Art. 9(1) nevertheless remain within reasonable limits. It should balance the right for data recipients to access data at affordable conditions with the protection of economic interests of data holders.

41. In line with the objective of promoting continued investment into data generation, a margin can be added on top of items that qualify as "investments in the collection and production of data" within the meaning of Article 9(2)(b). Recital 47 states that the margin may vary depending on data-related factors (e.g. volume, format, or nature), the costs of collection, the impact on the data holder's activities, and whether other parties contributed to data generation. Moreover, it states that the margin should be higher when data collection requires significant investment, lower when costs are minimal or the data is co-generated, and may be reduced or excluded if the data recipient's use does not impact the data holder's business.

42. In this context, the data holder may request information about the data recipient's intended use exclusively to assess whether its own activities are affected. To this end, the data holder may request the recipient to declare whether the use will compete with, replace, or interfere with the data holder's activities, which allows the data holder to determine if a margin is justified or if it should be reduced or excluded. The data holder cannot request or collect information irrelevant to the calculation of the margin, such as the data recipient's commercial plans, expected downstream profitability or market advantages, to justify a higher margin.

43. As a general rule in accordance with Article 9(2)(b), investments made in data collection and production should be taken into account for the calculation of the

reasonable compensation, including those made for the data holder's own purposes (Recital 47). There are, however, situations where investments should not be taken into account (wholly or partially), such as:

a. The investments have been depreciated/covered by another revenue source, notably the purchase price of a connected product or a related service. In the context of Chapter II of the Data Act, the acquirer or rentor/lessor of a connected product may – via the purchase price or the rent paid – have already covered any investments into data collecting or production functionalities, making it unreasonable for the data holder to require a data recipient to pay a compensation that includes such investments.

b. Under Chapter II of the Data Act, investment decisions to fit data collection or production technologies into connected products are made based on a purpose defined by the manufacturer (who is also, typically, the data holder). When the data holder itself uses the data, e.g. to monitor the connected product's performance, the margin is decreased (Recital 47). However, in situations where the manufacturer does not use the data and rather makes investments solely to enable additional data collection and production features, this can be included in the calculation of the margin. This may especially arise once Chapter II data sharing matures, and data recipients request data that is not needed for the functioning of the connected product or the manufacturer's or data holder's services.

c. Where a connected product is operated by a user, the operating costs should not be considered "investments in the collection and production of data" as such costs are borne by the user ("co-generation" referred to in Recital 47).

4.4. Specific elements when the data recipient is an SME or a not-for-profit research organisation

44. Article 9(4) of the Data Act grants preferential treatment to data recipients that are SMEs, or not-for-profit research organisations. This does not apply if such data recipients have a partner or linked enterprise that do not qualify as SMEs (Article 9(4)).

45. First, such data recipients can only be required to compensate the data holder for the *costs* incurred in making the data available. This results from Article 9(4) read in conjunction with Article 9(2)(a). As a consequence, the reasonable compensation to be requested from data recipients that are SMEs or not-for-profit research organisations cannot include a margin, as stated in Recital 47.

46. Second, Recital 49 of the Data Act specifies that the reasonable compensation to be paid by these data recipients should only be based on the costs directly related to making the data available for the individual request of each data recipient concerned. "Directly related costs" are costs that are attributable to the individual request, excluding the upfront and overhead costs that the data holder incurred in setting up the mechanisms necessary for sharing data, such as interfaces, related software, and connectivity. This needs to be considered when reading these Guidelines, and in particular section 4.1. on cost items under Article 9(2)(a).

5. COMPENSATION FORM AND INFORMATION

5.1. Determining the pro-rata share for each data recipient

47. For all cost and investment items that are one-off items (upfront and overhead costs), it will be necessary to calculate the reasonable share for each individual data recipient.

48. The Data Act obliges data holders to have a data access mechanism in place. Setting up such mechanism requires upfront investments, while the volume of access requests will vary and cannot be known in advance. This demand uncertainty is typical of business operations and should be anticipated and managed accordingly. Several strategies are possible to minimize exposure.[6] Data holders may, for instance:

    a. Define reasonable amortisation cycles, e.g. linked to the life span of technical equipment.

    b. Calculate the pro-rata share based on a conservative estimate of the number of prospective data recipients. If upfront and overhead costs are amortised earlier than expected, this should influence future calculation of compensation.

    c. Periodically adjust the compensation rates (e.g. on an annual basis) in such a manner that ensures clear pro-rata cost sharing and prevents discriminatory pricing over time. Periodic adjustments can risk creating a "first-mover disadvantage" if early data recipients are charged disproportionately higher amounts compared to later data recipients, which would conflict with the non-discrimination principle. Data holders should therefore ensure any adjustments are applied consistently and transparently.

5.2. Payment model

49. Besides the eligible cost and investment elements, the data holder and data recipient must also agree on the arrangements for paying compensation. The data holder may prefer a payment for each transaction or deploy subscription models – or both. Chapter III of the Data Act does not prescribe which model to use. Subscription models enable the distribution of onboarding and contracting costs across a larger number of transactions, making such models more cost-effective compared with per-transaction pricing.

50. A possible payment approach supported by stakeholders during the webinar is a hybrid structure that combines a base access fee with variable charges. The base (or minimum) fee covers integration and onboarding, ensuring initial costs are predictable. Usage is then priced by volume (e.g. per API call, per dataset, per user or device) with tiered data that lower the unit price as consumption increases.

51. There may be cases where reasonable compensation takes a non-monetary form instead of direct financial payment, such as access to services, reciprocal data sharing, or other forms of value that align with the parties' interests. The parties should always consider,

[6] See Section 4.1.4 of the Study for developing criteria for assessing "reasonable compensation" in the case of statutory data access right (2022) (cf. above, footnote 5).

when engaging in such non-monetary compensation forms, the non-discriminatory treatment of data recipients (see above, paragraphs 11–14 of the Guidelines) .

5.3. Transparency of the calculation and Article 9(7)

52. Article 9(7) allows a data recipient to request a data holder to provide "information setting out the basis for the calculation of the compensation in sufficient detail so that the data recipient can assess whether the requirements of paragraphs 1 to 4 are met". Unlike the elements that must be disclosed in a pre-contractual phase under Article 3(2) and (3),the function of Article 9(7) is not a general transparency obligation but a means to prevent abusive pricing practices by allowing for verification of the respect of the FRAND principle. Therefore, the information referred to in Article 9(7) should be given upon request only.

53. The recommendation is for data holders to disclose high-level cost categories early, publicly and more in depth during pre-contractual discussions. The information under Article 9(7) should be shared later, upon request, for instance, once the recipient is validated or has entered into a data sharing agreement. The data holder may provide the information under Article 9(7) through an independent third party. Data holders should be able to refuse to provide information in clearly abusive cases.

54. To comply with Article 9(7), data holders should to the extent necessary document the relevant policies and decisions on compensation, both the calculation in the abstract and individual decisions.

55. Data holders must provide information that sets out the basis for the calculation of the compensation in sufficient detail. Article 9(7) does not directly oblige data holders to disclose confidential information. Such information includes cost items protected by non-disclosure-agreements (e.g. on the cost of technology necessary for cloud storage or data transmission) or qualifying as trade secrets. Disclosure of such costs/prices may have unintended market effects and may adversely affect the data holder's business interests. For this reason, the data holder should provide information with the appropriate level of granularity, striking a balance between the protection of confidential information and the necessary transparency. A solution could be the creation of summaries, cost categories, or standard templates with example calculations, to show the logic of pricing and aggregated ranges rather than sensitive internal details (e.g. salaries, unit prices, supplier contracts). Where such information is not sufficient for the data recipient to assess whether the conditions of Article 9(1) to (4) have been met, or where there are grounds to challenge the calculation, the parties should strive for third-party intermediary solutions (e.g. independent auditors, dispute settlement bodies bodies) or other suitable measures (e.g. non-disclosure agreements) to allow for data recipients to challenge cost calculations while protecting commercially sensitive data.

56. Where the data holder and data recipient are actual or potential competitors, the provision by the data holder of cost information that goes beyond the requirements of Article 9(7) could constitute an exchange of commercially sensitive information

between competitors, contrary to Article 101 of the TFEU[7]. Where the parties are in such a competitive relationship, they can minimise the risk of infringing EU competition law[8] by, for example, (i) ensuring that the information provided is limited to what is necessary to comply with Article 9(7), and (ii) requiring the data recipient to use a 'clean team' to receive and process the information, namely a small group of individuals in the data recipient's organisation who are not involved in its commercial activities and are bound by strict confidentiality rules. For more structured guidance on information sharing between actual or potential competitors, parties can examine, inter alia, Chapter 6 of the Commission Guidelines on the applicability of Article 101 of the TFEU to horizontal co-operation agreements.[9]

6. ENFORCEMENT

57. When it comes to the resolution of disputes arising from the calculation of the reasonable compensation under Article 9 of the Data Act, data holders and data recipients have three options:

    a. They can seek redress before a court or tribunal of a Member State. The right to do so is not affected by having access to a dispute settlement body or by having filed a complaint with a national competent authority.
    b. The parties can also agree to refer the dispute to a dispute settlement body certified by Member States in accordance with Article 10 of the Data Act. Dispute settlement bodies should offer a simple, fast, and low-cost solution to the parties in addressing disputes relating to FRAND terms and conditions and transparently making the data available. Parties can address a dispute settlement body in any Member State.
    c. They can file a complaint with the competent authority designated by a Member State to carry out the tasks listed in Article 37(5) of the Data Act. Data holders and data recipients should lodge their complaints with the relevant competent authority in the Member State of their habitual residence, place of work or establishment, including with respect to cross-border matters. The competent authorities have a duty to cooperate and assist each other not only within the same Member State but also across borders.

[7] Article 101(1) TFEU prohibits anti-competitive agreements and concerted practices between undertakings.
[8] Where an undertaking discloses commercially sensitive information to its competitor, both undertakings can be liable for an infringement of Article 101 TFEU.
[9] Commission Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (OJ C 11, 14.1.2011, pp. 1-72)