Associazione Farmaceutici Industria
Società Scientifica

ASSOCIAZIONE FARMACEUTICI INDUSTRIA
SOCIETÀ SCIENTIFICA ETS

Response to the public consultation on the European Data Protection Board's Guidelines 02/2026 on anonymisation

Position Paper

29 October 2026

A.F.I. – V.le D. Ranzoni, 1 – 20149 Milano – Tel. 02.4045361 – 02.4047375 – Fax 02.48717573
E-mail: segreteria@afiscientifica.it – http://www.afiscientifica.it

Associazione Farmaceutici Industria
Società Scientifica

Document information

Document	Position Paper
Organisation	AFI – Associazione Farmaceutici Industria Società Scientifica ETS, Milan
Authors	Avv. Silvia Stefanelli, Avv. Laura Liguori, Avv. Maddalena Collini, Dr.ssa Arianna Avitabile, Dr.ssa Sara Cazzaniga, Dr.ssa Ilaria Maruti and Dr. Lorenzo Cottini
Date	29 October 2026
Version	1.0
Document commented on	EDPB, Guidelines 02/2026 on Anonymisation, version 1.0, adopted on 7 July 2026 (version for public consultation)
Procedure	EDPB public consultation
Language	English
Contact	AFI administrative (segreteria@afiscientifica.it)

Contents

Contents

CONTENTS **3**

1. ABOUT AFI **4**

2. EXECUTIVE SUMMARY **5**

3. DETAILED COMMENTS **7**

3.1 SECTION 1 · INTRODUCTION 7
3.2 SECTION 2.1 · LEGAL ANALYSIS – INTRODUCTION 8
3.3 SECTION 2.2 · IDENTIFYING THE APPLICABLE PERSPECTIVE(S) 11
3.4 SECTION 2.4 · WHETHER THE NATURAL PERSON IS "IDENTIFIED OR IDENTIFIABLE" 12
3.5 SECTION 2.4.2 · MEANS REASONABLY LIKELY TO BE USED 13
3.6 SECTION 2.5 · ADDITIONAL CONSIDERATIONS 19
3.7 SECTION 3.4.3 · NO INFERENCE 21
3.8 SECTION 3.5 · APPLYING THE CRITERIA 23
3.9 CONCLUDING REMARK · THE CONTROLLER'S ROLE CANNOT PRECLUDE ANONYMISATION 27

4. BIBLIOGRAPHY **29**

1. About AFI

AFI, Associazione Farmaceutici dell'Industria, is a scientific society founded in 1960 and based in Milan. It brings together professionals and companies from the pharmaceutical, chemical, dietetic, food, cosmetic and related sectors. By ministerial decree of 23 September 2021, it was included in the list of scientific societies and technical-scientific associations of the health professions kept by the Ministry of Health. Its areas of interest include research and development, clinical matters, regulatory affairs and medical devices.

The Guidelines are of direct interest to AFI's members, as they are involved in researching and devoloping medicinal products and medical devices and making them available to patients, and process health data in these activities.

2. Executive Summary

AFI welcomes the publication of Guidelines 02/2026 on anonymisation, adopted by the European Data Protection Board on 7 July 2026, which update Opinion 05/2014 of the Article 29 Working Party.

AFI shares the basic approach of the document. The relative approach, which stems from the judgment of the Court of Justice of 4 September 2025, Case C-413/23 P, EDPS v SRB, recognises that the same data may be personal for one entity and anonymous for another (paragraphs 6 and 7).

AFI's comments concern how this approach is applied and the operational guidance that the anonymising entity needs.

AFI's comments and requests aim to make the Guidelines applicable by organisations of every size, and to enable the anonymising entity to document its assessment in a verifiable way, as required by paragraph 41.

*

The summary below sets out the main comments, grouped by theme.

Chapter 3 develops the detailed comments: for each point it identifies the paragraph of the Guidelines and reproduces its text, sets out AFI's comments and the proposed amendment and, where AFI puts one forward, the proposed wording.

*

Main comments

1. Link with the EHDS and the Data Act

paragraphs 2 and 34

The Guidelines do not coordinate with Regulation (EU) 2025/327 on the European Health Data Space (EHDS) or with Regulation (EU) 2023/2854 (Data Act). While the EHDS makes anonymisation the rule for the secondary use of health data, requires secure processing environments from which only non-personal data may leave, and prohibits re-identification, with penalties of up to 4% of total worldwide annual turnover, the Guidelines do not appear to take this vision into account.

AFI asks for a dedicated section clarifying the relationship between the qualification of the data made by the health data access body and the assessment of the anonymous nature of the data required of the entity that receives them.

2. The role of the controller and the anonymisation and sharing chain

paragraphs 4, 7, 12, 15 and 37; concluding remark

The issue is cross-cutting. The role of controller risks becoming the starting point for denying anonymity, whereas it should be its consequence (paragraph 4). The text leaves it unclear whether a provider acting on behalf of the controller, with no means of identification whatsoever, is subject in every respect to the rules on personal data, including the rules on transfers to third countries (paragraph 15). It is not clear who must reassess anonymity each time the data are communicated anew (paragraph 12), nor what obligations remain for the anonymising controller when the data remain personal from its perspective (paragraphs 7 and 37). Finally, the Guidelines

do not address anonymisation at source by those who collect the data, using tools provided by the party proposing the research project. Without an express position, anonymisation would become impossible for anyone promoting a project, solely by virtue of the role they hold.

3. Means reasonably likely to be used: security, legal prohibitions and organisational measures

paragraphs 9, 21, 26, 29-34, 89, 90 and example 22

AFI asks that two choices it shares be retained in the text: the threshold of reasonably likely transfer to a third party (paragraph 21) and disproportionate effort as a standalone scenario, distinct from practical impossibility, for which it asks for measurement parameters (paragraph 26). It then asks for clarification of the relationship between the legal prohibition and unauthorised access to systems: for attackers the presumption of compliance with the law almost never operates, but the likelihood of success nonetheless depends on the security measures adopted (paragraphs 32, 33 and 89). It asks for clarification of who bears the burden of proving a concrete re-identification risk (paragraph 33) and for specific weight to be given to verified and documented technical and organisational measures, which the draft relegates to a complementary role (paragraphs 29, 34 and 90). It points out the inconsistency between paragraph 89, under which, with adequate security controls, unauthorised access is not a means reasonably likely to be used, and example 22, which nonetheless includes those who breach the system despite state-of-the-art measures. Finally, it asks for a method to select the relevant entities and for a distinction between subjective motivation and objective interest in re-identification (paragraphs 9, 30 and 31).

4. Methodological continuity and operational techniques

paragraphs 28, 36, 71, 77, 82, 87, 91 and 98

AFI asks for a correspondence table between the triad of singling out, linkability and inference of Opinion 05/2014 and the three criteria of the Guidelines, with guidance on updating assessments already carried out (paragraphs 28 and 98). It asks for operational guidance on AI models and synthetic data, already widely used in the sector for conducting research and studies, with a structured cross-reference to the Board's Opinion 28/2024 (paragraphs 77 and 82). It also asks for an alignment between the inference verification method and the statistical techniques in use (paragraph 71), and for worked examples on hashing and k-anonymity, i.e. the most widely used techniques (paragraph 91). Finally, it asks for criteria for the separate treatment of mixed datasets, which are particularly relevant for rare disease research, where some isolable records are structural (paragraphs 36 and 87).

5. Review of anonymity over time and security incidents

paragraphs 35, 42 and 88

The Guidelines recommend periodic reassessment, adequate safety margins and a new assessment after a security incident. However, they do not indicate when and how often to proceed, who should carry out the assessment (especially after the data have been shared with several recipients), what level of protection suffices to maintain anonymity and what effects a negative outcome has on analyses and publications already carried out and concluded. For multi-year studies, these elements are essential for activity planning.

3. Detailed comments

The comments below follow the order of the Guidelines. For each point, the paragraph concerned and its text are given, followed by AFI's comments, the proposed amendment and, where applicable, the proposed wording.

The concluding remark (section 3.9) concerns the relationship between the role of controller and the anonymous nature of data, a theme that runs through several sections.

3.1 Section 1 · Introduction

§ 2 Link with the EHDS and the Data Act

> **Guidelines 02/2026, paragraph 2**
> *"The Article 29 Working Party Opinion 05/2014 on anonymisation techniques was published in 2014 and provided three criteria for assessing the anonymity of data. Since then, however, there have been major changes in the legal, privacy, engineering and technological landscapes. The development of case law from the Court of Justice of the European Union (CJEU), the establishment of EU-wide data spaces, and developments in both AI and technology in general, amongst many other things, have raised a need to update that Opinion and refine the criteria presented there. These guidelines provide that update, together with further guidance on the topic."*

AFI'S COMMENTS

The EDPB states that the creation of EU-level data spaces is among the reasons requiring the update of Opinion 05/2014. However, the Guidelines provide for no coordination or harmonisation with the EHDS framework.

The EHDS assigns anonymisation a central role in the secondary use of health data. Article 66, (par. 2) provides that the access body is to supply anonymous data where the purpose can be achieved with them; Article 73 requires secure processing environments; Article 61(par.3) prohibits re-identification, with penalties of up to EUR 20 million or 4% of total worldwide annual turnover (Article 64(par.5)).

Without a clear link between the two frameworks, those who receive data qualified as anonymous by the health data access body risk having to repeat the assessment using different criteria and reaching the opposite conclusion. Clarification on this point would give certainty to researchers, companies and data access bodies.

PROPOSED AMENDMENT

AFI proposes adding a dedicated section on the relationship between the Guidelines and the sector-specific Union frameworks, in particular Regulation (EU) 2025/327 (EHDS) and Regulation (EU) 2023/2854 (Data Act), cross-referring to it in paragraph 2, which already cites European data spaces among the reasons for the update.

The section should clarify: (i) whether compliance with the conditions of Articles 66 and 73 of Regulation (EU) 2025/327 is relevant to the anonymity assessment; (ii) what relevance the qualification of the data made by the health data access body has for the data user; (iii) that the

prohibition on re-identification in Article 61(par.3), backed by the penalties in Article 64(par.5), constitutes a legal prohibition within the meaning of paragraphs 32 and 33.

§ 4 Role of the controller

> **Guidelines 02/2026, paragraph 4**
> *"Much of the content in these guidelines sits in the space between anonymous and personal data – since the guidelines set out criteria for testing whether a dataset falls into one side or the other, they adopt some terminology specific for these guidelines. It is not possible, for example, to know if the person holding the data should be described as a controller or not, since that answer will depend on whether the data being tested is personal or not. Therefore, rather than, for example, constantly referring to "the person who may or may not be a controller", these guidelines use a number of key terms for the sake of readability, all of which are set out in more detail in a glossary at the end of this document."*

AFI'S COMMENTS

Paragraph 4 correctly states that it cannot be known in advance whether the holder of the data is a controller, because the answer depends on the nature – personal or not – of the data concerned. In practice, the reasoning tends to be inverted: an entity is qualified as controller, and it is inferred that the data are personal for it.

An explicit sentence would help the interpreter follow the correct logical order: first, it is established for whom the data are personal; then roles are assigned. The amendment would make the paragraph consistent with the relative approach of paragraphs 6-7.

PROPOSED AMENDMENT

AFI shares the principle of paragraph 4 and proposes adding, at the end of the paragraph, the sentence below.

> **Wording proposed by AFI**
> "The attribution of the role of controller to an entity does not in itself determine the personal nature of the data it receives after anonymisation. That nature depends on the means reasonably likely to be used by that entity, in accordance with paragraphs 6-7 and 11-12."

Reference is also made to the concluding remark on the role of the controller (section 3.9).

3.2 Section 2.1 · Legal analysis – Introduction

§ 6 Relative approach

> **Guidelines 02/2026, paragraph 6**
> *"The core test for anonymity asks two questions:*
>
> *a. Does the information "relate" to a natural person? If so,*

> *b. Is that natural person "identified or identifiable"?*
>
> *If the answer to either of these questions is "no", then the data should be considered anonymous. Importantly, these answers may vary from one entity to another. This means that information may be anonymous for some entities, but not for others."*

AFI'S COMMENTS

The relative approach stems from the judgment of the Court of Justice of 4 September 2025, Case C-413/23 P, EDPS v SRB. It allows anonymity to be assessed for each entity on the basis of the means it can reasonably use. It prevents the same data from being treated as personal for entities that have no means of identification whatsoever.

AFI shares this approach and proposes keeping paragraph 6 in its current wording.

The comments below concern only how this approach is applied in the following paragraphs.

§ 7 Anonymity for the anonymising controller

> **Guidelines 02/2026, paragraph 7**
> *"For example, information may unambiguously relate to an individual, but only one organisation may be able to actually identify that individual. In this case, the answer to both questions would be "yes" from that organisation's perspective, and so the information would be considered personal data for that organisation. At the same time, the answer to the second question would – outside of particular circumstances that will be explained later – be "no" from everyone else's perspective, and so the information would be considered anonymous for everyone else. It is, therefore, necessary to consider the different perspectives of the relevant entities when performing this test. This means that anonymisation can be done in a way that the data is anonymous for everyone, or in a way that is only anonymous for particular entities (which may or may not include the anonymising controller)."*

AFI'S COMMENTS

It is not clear under what conditions the data may be considered anonymous also for the controller that carried out the anonymisation.

Indeed, paragraph 7 accepts that data may be anonymous for some entities but not for others, among which may be the controller that anonymises them; however, the conditions under which this may occur are not indicated. Paragraph 10 adds that anonymisation is possible even without deleting the original data; example 22, however, addresses only the case in which the original data are deleted.

In research, it is essential to know when the controller carrying out the anonymisation may consider the data anonymous also for itself, both where the original data are deleted and where they remain with another entity and the controller has no access to them. This is because many research projects separate those who produce the data from those who receive them in anonymous form: for these cases, certain and verifiable criteria are needed, enabling every assessment to be documented.

PROPOSED AMENDMENT

AFI asks that a further example be given, after paragraph 7, illustrating the conditions under which anonymised data may be considered anonymous also from the perspective of the controller that carried out the anonymisation, in particular where the original data are deleted or remain with another entity to which the controller has no access. The example should set out the conditions under which the data are anonymous also from that controller's perspective, such as the absence of access to the original data and to additional information, the separation between the entities and the independent verification of the technique used to anonymise the data.

Reference is made to the concluding remark (section 3.9).

§ 9 Relevant entities

> **Guidelines 02/2026, paragraph 9**
> *"It should also be recognised that these questions assume that the entity in question has, or could have, some kind of access to, or control over, the data. If, taking into account the means that the entity is reasonably likely to use, an entity cannot actually access or process the data, is not meaningfully connected to any other entities (or chain of entities) with such access, and is not likely to receive the data from such other entities, then it should not be necessary to assess whether the information is anonymous for that entity."*

AFI'S COMMENTS

Paragraph 9 provides that there is no need to assess the perspective of an entity that reasonably: (i) cannot access the data, (ii) is not meaningfully connected to those who do, and (iii) is not likely to receive them. Paragraph 30 lists highly heterogeneous categories of entities, going as far as citing foreign intelligence services, but does not refer to the criterion in paragraph 9 and does not explain the relationship between the two paragraphs. Such a cross-reference would give the operator a method for choosing the categories to consider and would thus make the reading of the two paragraphs coherent.

PROPOSED AMENDMENT

AFI proposes referring to the criterion of paragraph 9 in paragraph 30, by adding to the latter a sentence along these lines.

> **Wording proposed by AFI**
> "The following list is indicative. Only those categories of entities are relevant which, under the criterion of paragraph 9, can reasonably access the data, are meaningfully connected to those who access it, or may receive it."

3.3 Section 2.2 · Identifying the applicable perspective(s)

§ 12 Further communications of the data

> **Guidelines 02/2026, paragraph 12**
> *"It can sometimes be immediately apparent if a certain entity is relevant or not. The basic question is: for whom is the data intended to be anonymous? For example, if the intention is to anonymise data for an entity's own use, that entity's perspective will be relevant for the assessment. Likewise, if the intention is to anonymise the data for independent use by anyone who receives the data, anonymity should generally be assessed from the perspective of those who will have access to the data after it has been transferred. In some cases, there may only be one relevant perspective (e.g., if the data is kept securely by a single entity and nobody else will ever be able to gain access to it) while, in others, there may be many different relevant perspectives (e.g., if the data could be accessed by many entities)."*

AFI'S COMMENTS

Paragraph 12 provides that, where the data are intended for the independent use of those who receive them, anonymity is assessed from the perspective of those who will have access to them after the transfer. However, the text does not say who must carry out the anonymity assessment for each new recipient. The point is essential, since in research the data circulates among several partners. Accordingly, responsibility for carrying out the anonymity assessment should be identifiable in advance, so that it can be carried out and properly documented, as required by paragraph 41.

PROPOSED AMENDMENT

AFI proposes clarifying, in paragraph 12 or in a later paragraph, what happens when anonymous data are communicated to a new recipient, and in particular: (i) whether the communication requires a new assessment from the recipient's perspective; (ii) which entity is responsible for carrying it out, among the one that anonymised, the one that transfers the data and the one that receives them; (iii) how that assessment is coordinated with the periodic reassessment in paragraph 35.

§ 15 Provider without means of identification

> **Guidelines 02/2026, paragraph 15**
> *"Importantly, the applicable perspective used for a particular entity depends on whether they themselves determine the means and purposes of the processing. If an entity processes information on behalf of another, whether the given data is personal for that entity should be assessed by reference to the controlling entity's perspective. In practice, this means that if an entity processes information on behalf of a controller (i.e. someone for whom the information is personal data, and who decides the purposes and means of the processing), that information should also be considered personal data for the processing entity. That entity should, therefore, be considered a processor under the GDPR and be subject to the obligations applicable to processors. This follows from a teleological application of the GDPR, noting that: […]"*

AFI'S COMMENTS

Paragraph 15 presents the rule as a teleological application of the GDPR: whoever processes data on behalf of a controller adopts the controller's perspective: if the data are personal for the latter, they are also personal for the provider, which becomes a processor under Article 28 GDPR. However, neither the text nor the examples clarify the consequences of the following scenario: does this rule also apply to a provider that, for technical reasons, is unable to identify the data subjects? The case concerns in particular data processing platforms, including those established outside the Union, that process encrypted or aggregated data. If the data must be considered personal, for all purposes, also for the provider, the rules on transfers (Article 44 et seq. GDPR) would then also apply, with burdens disproportionate to the actual risk.

PROPOSED AMENDMENT

AFI proposes clarifying, in paragraph 15, whether the rule also applies to a provider that, for technical reasons, is unable to identify the data subjects.

AFI also proposes adding an example concerning a data processing environment in which the provider has no means of identification whatsoever, such as in the case of data encrypted with keys held solely by the controller, federated analysis or a data clean room.

3.4 Section 2.4 · Whether the natural person is "identified or identifiable"

§ 21 Transfer of anonymous data to third parties

> **Guidelines 02/2026, paragraph 21**
> *"In this regard, the EDPB emphasises that if (a) it is reasonably likely that an entity can transfer the data to a third party, and (b) it cannot be ruled out that this receiving entity has the means to identify the individual through means reasonably likely to be used, the data should be considered personal for both that transfer and for any subsequent processing of the data by that recipient. Further, this transfer means that the transferred information would also indirectly become personal for the transferring entity, even if that entity would not otherwise have means reasonably likely to be used to identify the individuals in question."*

AFI'S COMMENTS

The probability condition prevents a merely possible or hypothetical step from making otherwise anonymous data personal. It is consistent with the criterion in Recital 26 GDPR, which requires consideration of the means reasonably likely to be used. Indicating the elements of probability makes the assessment predictable and capable of being documented under paragraph 41.

PROPOSED AMENDMENT

AFI proposes supplementing the paragraph with an indication of the elements to be considered that make a transfer likely, such as the provision for communication in the project, cooperation between the entities and the existence of a legal obligation to communicate the data.

3.5 Section 2.4.2 · Means reasonably likely to be used

§ 26 Disproportionate effort

> **Guidelines 02/2026, paragraph 26**
> *"Rather than describing which means are reasonably likely to be used per se, the CJEU has defined this concept by reference to things which would stop means from being reasonably likely to be used by a particular entity. In particular, means may not be reasonably likely to be used if the likelihood of identification appears, in reality, to be insignificant because it would be impossible to do; because it would involve disproportionate effort in terms of time, cost and labour; or because of a legal prohibition. This sub-section provides further guidance on this concept and on how to assess whether a means can be considered reasonably likely to be used or not."*

AFI'S COMMENTS

In research, re-identification is almost always theoretically possible, but requires resources, skills and additional information that, in practice, no entity involved in the research project would use or have an interest in using. Paragraph 26, in line with the case law cited in footnotes 19 and 20, recognises this criterion. However, paragraphs 92 and 93 state that the use of re-identification techniques is becoming increasingly accessible, because it requires limited resources and can be carried out within a reasonable time. It is therefore unclear to the operator how to interpret these provisions, since it cannot know when the effort is disproportionate. The criterion risks remaining without application.

PROPOSED AMENDMENT

AFI proposes confirming that disproportionate effort (in terms of time, cost and resources) is one of the scenarios in which a means is not reasonably likely to be used, and supplementing the paragraph with: (i) the parameters to measure it, such as time, cost, skills and resources required and the availability of additional information; (ii) an example relating to scientific research; (iii) an alignment with paragraphs 92 and 93, which treat time and cost as factors that are normally not prohibitive, clarifying how disproportionate effort is to be assessed in light of those paragraphs.

§ 28 Concept of means and continuity with Opinion 05/2014

> **Guidelines 02/2026, paragraph 28**
> *"The concept of "means" should be understood broadly, covering anything from simply reading a document to making a web search to running incredibly complex analyses and inferences. Further, an entity's means can also include taking advantage of means that are available to another entity; where this is possible, it is important to assess the likelihood that this overall "chain" of means comes together."*

AFI'S COMMENTS

Opinion 05/2014 built the assessment on three risks: singling out, linkability and inference. Recital 26 GDPR follows the same approach, indicating singling out as a typical means. The Guidelines adopt the criteria No Record Isolation, No Linkage and No Inference and address singling out at paragraphs 54 and 98, without explaining the relationship with the earlier terminology.

In addition, footnote 3 dispenses with redoing assessments already carried out, but does not indicate how to update them.

PROPOSED AMENDMENT

AFI proposes: (i) referring, in section 2.4.2, to Recital 26 GDPR, which indicates singling out as an example of a means; (ii) clarifying that singling out, linkability and inference, as developed in Opinion 05/2014, remain relevant modes of identification for the purposes of the GDPR; (iii) making explicit the relationship between these means and the three criteria of section 3.4; (iv) inserting a correspondence table between the terminology of Opinion 05/2014 and that of the Guidelines; (v) indicating how to update assessments already carried out under Opinion 05/2014, referred to in footnote 3.

§ 29 Access restrictions

> **Guidelines 02/2026, paragraph 29**
> *"Whether an entity is likely to use certain means to identify an individual should be assessed in light of all objective factors that might influence the availability of such means and the likelihood of their actual use, including:*
>
> *a. the properties of the data itself – including whether the data is aggregated, the uniqueness of the records, as well as the accuracy and precision of the information – and how these affect the data's vulnerability to the different possible means of (re-) identification;*
> *b. the context in which the data are released and/or processed, including whether there are any effective and permanent restrictions on access to the data;*
> *c. any additional information that would allow for the identification of individuals, and how likely it is that such information can be obtained;*
> *d. the costs and the amount of time that the entity would need to obtain such additional information (in case it is not already available to them); and*
> *e. the available technology at the time of the processing, as well as reasonably foreseeable technological developments.*
>
> *Notably, if the law provides means to access additional information, it is objectively clear that such access constitutes a means reasonably likely to be used."*

AFI'S COMMENTS

Point (b) includes among the objective factors of the assessment the existence of effective and permanent restrictions on access to the data. Paragraphs 34 and 90, which address technical, organisational and contractual measures, seem to deny these measures any autonomous weight. Aligning the two paragraphs would remove the uncertainty and allow operators to understand and assess every relevant aspect in the assessment.

PROPOSED AMENDMENT

AFI proposes clarifying, in paragraph 29, point (b), that effective and permanent access restrictions include technical and organisational measures subject to independent and documented verification, and aligning paragraphs 34 and 90 with that point.

§ 30 Selection of relevant entities

Guidelines 02/2026, paragraph 30
"The GDPR does not lay down any conditions regarding the entities who are able to identify the individual. Relevant entities may, therefore, include anybody directly or indirectly receiving the data, including unauthorised and malicious actors. Depending on the circumstances at hand, these may include (among others): […]"

AFI'S COMMENTS

Footnote 25 specifies that not all categories are to be considered systematically, but the text does not indicate in which circumstances. Without a clear indication, the prudent operator will always treat the data as personal. Those that are not highly structured, or that have no corporate threat-analysis functions, will omit the categories they do not know how to assess, with the result that the assessment will be incomplete and difficult to document under paragraph 41. A selection method would enable complete and reliable assessments, even for medium-sized organisations.

PROPOSED AMENDMENT

AFI proposes that paragraph 30, or the following paragraph, set out the factors that make each category of entity relevant or not relevant: (i) the likelihood of access to the data by reason of the distribution channel; (ii) the availability, within that category, of the necessary additional information; (iii) the typical interest in that type of data.

AFI also proposes reordering the list according to those factors, referring to the criterion of paragraph 9 and clarifying how the chain of means affects selection.

It is also asked to clarify how an entity must and may consider and assess the following categories: (i) national law enforcement authorities or intelligence agencies; (ii) foreign intelligence services; (iii) cybercriminals.

§ 31 Motivation and interest in re-identification

Guidelines 02/2026, paragraph 31
"The EDPB cautions against using "lack of motivation" as a factor in this analysis. As a starting point, the motivation of individuals can be difficult to assess or demonstrate objectively and may change over time. Moreover, an entity's actions may not be consistent with their motivations. It may be, for example, that identification occurs due to an accident or negligence. This could also happen if an entity is forced by outside circumstances to identify an individual, or to transfer information which allows for such identification. When assessing the means reasonably likely to be used, the potential value of the re-identified data to the re-identifying entity (which is not limited to monetary value) should be taken into account to the extent that it offsets the costs and effort involved in re-identification. Equally, the risks that re-identification entails for the re-identifying entity should be considered in the context of this assessment."

AFI'S COMMENTS

Paragraph 31 advises against treating lack of motivation as a relevant factor in the analysis but then asks for an assessment of the value of the re-identified data against costs, effort and risks. On closer inspection, these elements measure in concrete terms precisely the interest or motivation to re-identify. If the text does not distinguish between subjective motivation and objective interest, the operator does not know what it is supposed to assess in concrete terms.

PROPOSED AMENDMENT

AFI proposes clarifying that paragraph 31 excludes the relevance of subjective motivation, whether declared or presumed, and not the objective analysis of the interest in re-identifying. AFI proposes expressly referring to the objective parameters in the second part of the paragraph (value of the re-identified data, costs, effort and risks for the person re-identifying) and also indicating how to document them.

§ 32 Legal prohibition and unauthorised access to systems

> **Guidelines 02/2026, paragraph 32**
> *"The CJEU has stated that means do not need to be considered if, in reality, the likelihood of their use is insignificant because they are prohibited by law. It should be noted that these cases involved actors who were properly limited by the rule of law, so that the law effectively prevented the use of the means in question. Indeed, we can generally assume that people will follow the law. However, there may also be cases where illegality does not provide any meaningful barrier to identification, because the entities involved will not actually be restricted by this prohibition."*

AFI'S COMMENTS

Paragraph 32 excludes means prohibited by law only with regard to those bound by the prohibition. It is also stated, however, that for unauthorised access to systems prohibition is not a barrier for attackers. The likelihood that access succeeds, however, depends on protective measures, as paragraph 89 and the third indicator of paragraph 33 show, the latter considering data particularly vulnerable for lack of protection. Example 8 confirms that improved security allows anonymity to be reassessed. If adequate and verified measures did not affect the assessment, no dataset could qualify as anonymous with regard to external attackers and investment in security would lose all relevance.

PROPOSED AMENDMENT

AFI proposes clarifying the relationship between paragraphs 30, 32, 33 and 89 with regard to unauthorised access to systems. In particular, AFI proposes specifying that, where the controller has adopted adequate security measures under Article 32 GDPR, documented and subject to verification, unauthorised access by unauthorised persons is not a means reasonably likely to be used, unless the evidence of a concrete risk indicated in paragraph 33 is present. AFI proposes adding an example to that effect.

§ 33 Burden of proof

Guidelines 02/2026, paragraph 33
"The general assumption that people will follow the law can, therefore, be rebutted if there is sufficient evidence of a concrete risk that unlawful means are nevertheless reasonably likely to be used. The assessment of this risk should consider evidence that the prohibition in question is not respected by the entities involved. Relevant factors may include, but are not limited to:

– evidence that the legal prohibition is not effectively monitored, enforced and sufficiently dissuasive;

– evidence that the gains from breaking the legal prohibition might outweigh costs, effort and potential risks of doing so;

– evidence of a situation where data relevant for re-identification (i.e. both the given and, potentially, the additional data useful for re-identification) is especially vulnerable to illegal access using the prohibited means, due to a lack of protection; and

– evidence that the prohibition has previously been breached or circumvented in comparable situations."

AFI'S COMMENTS

Paragraph 33 allows the presumption of compliance with the law to be overcome if there is sufficient evidence of a concrete risk, assessed on four indicators. However, the text does not indicate who must provide the evidence. The allocation of the burden of proof affects the documentation to be prepared and the defence in the event of a challenge.

PROPOSED AMENDMENT

AFI proposes specifying who is to provide the "sufficient evidence" referred to in paragraph 33 and whether the controller is required to demonstrate the absence of the indicators listed there or only to document its assessment under paragraph 41.

§ 34 Contractual and organisational measures

Guidelines 02/2026, paragraph 34
"A prohibition set out in a contract (even if it is legally binding upon its parties) should not be treated as a prohibition by law. While contractual terms may have an effect on the means reasonably likely to be used, they should only be used to complement technical measures, and it is important to carefully consider the actual strength of their effect. Among other things, the measures should be reliable, verifiable and enforceable, bearing in mind that contractual measures can typically be subject to revision, or may even be disregarded entirely by the parties."

AFI'S COMMENTS

AFI shares the principle of paragraph 34, whereby a contractual prohibition is not a legal prohibition, and that contractual clauses constitute organisational measures that serve to complement technical security measures. However, the paragraph treats contractual and organisational measures as a single category, with the consequence that a clause prohibiting the recipient from re-identifying the data,

without other safeguards, receives the same treatment as an articulated protection system (with a closed processing environment, named and logged access, keys held by a different entity, export of aggregated results only and periodic audits). What reduces the likelihood of re-identification is the set of measures, especially if an independent party has verified their operation. The paragraph also requires that measures be "reliable, verifiable and enforceable", but does not explain when these requirements are met. It does not clarify how to demonstrate them, nor who must verify them. Those who invest in verified protection systems therefore have no certainty that the anonymity assessment will take them into account.

The clarification is also needed for consistency with Regulation (EU) 2025/327. The EHDS makes health data usable for secondary use through a secure processing environment (Article 73) and a prohibition of re-identification laid down by law (Article 61(par.3)). The Union legislator, too, therefore recognises that a set of controlled technical and organisational measures affects the likelihood of re-identification.

PROPOSED AMENDMENT

AFI proposes that paragraphs 34 and 90 distinguish three situations: (i) the isolated contractual prohibition, without autonomous relevance; (ii) organisational measures that are declared but not verified; (iii) the set of technical and organisational measures subject to independent and documented verification, to which specific weight in the assessment should be given. AFI proposes setting out the requirements that make a measure "reliable, verifiable and enforceable", such as the closed environment, named and logged access, separate keys, export of aggregates only and periodic audits, indicating who verifies and with what evidence. AFI also proposes clarifying that re-identification prohibitions laid down by Union law fall within paragraphs 32 and 33.

§ 35 Periodic reassessment

> **Guidelines 02/2026, paragraph 35**
> *"Finally, the likelihood of re-identification typically increases over time due to advances in the technology and techniques used for re-identification, as well as the increased availability of additional information. If the likelihood of identification increases to a level that is no longer insignificant, the previously anonymous data should again be considered personal, and the controller will be accountable for any processing of that personal data. It is, therefore, good practice for entities processing anonymised data, wherever possible and as appropriate, to periodically reassess the likelihood of re-identification."*

AFI'S COMMENTS

Paragraph 35 indicates periodic reassessment as good practice, but does not say when and how often it must be carried out, nor who must carry it out, especially in cases where data are shared with several recipients. The text gives no indication regarding assessments already concluded. In research, for example for multi-year studies, certainty on these points is necessary to plan activities and to avoid reopening results already finalised.

PROPOSED AMENDMENT

AFI proposes indicating: (i) the events requiring an early review, such as a security incident, a new re-identification technique applicable to the data or an expansion of recipients; (ii) a minimum reference frequency; (iii) the allocation of obligations between those who anonymised and those who received the data; (iv) the consequences of a negative outcome for processing, analyses and publications already concluded.

3.6 Section 2.5 · Additional considerations

§ 36 Mixed datasets and rare diseases

> **Guidelines 02/2026, paragraph 36**
> *"Some anonymisation techniques might only make the likelihood of identification insignificant for some individuals in a dataset. In such cases, it is important to distinguish between the anonymity of records and the anonymity of the dataset per se. In particular, the dataset as a whole should only be considered anonymous if the anonymisation is effective for all of the included individuals – this does not necessarily require an equal level of protection for all individuals but does require the likelihood of re-identification to be insignificant for all of these individuals. Where this is not the case, and so a dataset contains a mix of personal and anonymous data, the entire dataset should be treated as containing personal data (and therefore within the scope of the GDPR) in any situation where the separate parts of the dataset are not treated separately."*

AFI'S COMMENTS

Paragraph 36 qualifies the whole dataset as anonymous only if it is so for all data subjects; otherwise, it must be treated entirely as personal data, and this in all cases where the parts of the dataset are not handled separately.

The text does not say, however, what it means to treat them separately. Without precise criteria explaining what such separation consists of, the whole dataset falls within the scope of the GDPR, even if almost all the records are anonymous. The difference between the text of the paragraph and that of footnote 31, which refers to the Meta Platforms judgment (Case C-252/21, paragraph 89), changes the meaning of the rule. The wording of the footnote, referring to the possibility of separating the parts, is clearer.

In research, especially rare disease research, some isolable records are unavoidable.

PROPOSED AMENDMENT

AFI proposes: (i) specifying the requirements for separating the parts of a mixed dataset, such as logical separation of access, physical separation and separation of permissions; (ii) aligning paragraph 36 with footnote 31, which refers to parts that "cannot" be treated separately, whereas the paragraph uses the expression "are not treated" separately; (iii) adding an example concerning a dataset in which a minority of records remains isolable and the parts are treated separately; (iv) coordinating the paragraph with paragraph 87.

§ 37 Obligations of the anonymising controller

> **Guidelines 02/2026, paragraph 37**
> *"The EDPB emphasises that when making information anonymous from some perspectives but not others, it is important to consider the possible implications for GDPR compliance. For example, when information is anonymised for the entity which receives the given data, but not for the anonymising controller, that controller will still have to treat the given data as personal data and comply with all of their GDPR obligations in regard to it."*

AFI'S COMMENTS

Paragraph 37 states that a controller for which the data remains personal must comply with all GDPR obligations. The text does not clarify whether those who collect and then anonymise the data can exit the personal-data regime for the resulting data, nor under what conditions. Paragraph 10 admits anonymisation without deletion of the originals. Paragraph 39 considers deletion only as a favourable factor in the legitimate interest balancing. However, clear criteria linking these indications and allowing the operator to find its bearings are lacking.

PROPOSED AMENDMENT

AFI proposes clarifying which GDPR obligations remain for the controller that carried out the anonymisation when the data remain personal from its perspective and specifying in which cases the resulting data are anonymous also for it, referring to paragraph 10 (anonymisation without deletion of the original data) and example 22 (anonymisation with deletion).

Reference is made to the concluding remark (section 3.9).

§ 42 Security incidents

> **Guidelines 02/2026, paragraph 42**
> *"In some cases, a security incident may lead to a reassessment of anonymity. This is particularly the case if the assessment of anonymity relied on certain information being kept confidential, but the incident means that the individuals can now be identified with means reasonably likely to be used. Where this is the case, the entity which suffered the incident should then determine its role with respect to the processing and whether it needs to fulfil any obligations under Article 33 and 34 GDPR."*

AFI'S COMMENTS

Paragraph 42 provides that a security incident may require anonymity to be reassessed where the assessment relied on the confidentiality of certain information, with the resulting obligations under Articles 33 and 34 GDPR. The anonymity assessment thus also becomes a security assessment, without the required level of protection being indicated. Those who have already used the data as anonymous should know in advance what consequences a potential incident could have on concluded activities and work carried out on anonymous data.

PROPOSED AMENDMENT

AFI proposes indicating what level of protection is sufficient to maintain the status of anonymous data, with reference to adequate, documented and verified security measures, and what consequences the

reassessment of the qualification of the data, following an incident, has on processing, analyses and publications already concluded.

AFI proposes coordinating the paragraph with paragraph 35.

3.7 Section 3.4.3 · No Inference

§ 71 Inference verification method

> **Guidelines 02/2026, paragraph 71**
> *"To consider that the given data actually relates to an individual, the inference should be specific and meaningful. This means that the inference will result in personal data whose processing is liable to have an effect on the data subject's rights and interests, relies on the given data and could not be obtained from general knowledge or from data about the population at large. This can typically be shown in one of three ways:*
>
> *b. If this is not possible, e.g. due to the opacity of automated processing that led to the inferred information, a lack of reliance could also be shown by comparing the outcome of inference with two versions of the given data – one which was produced from the original dataset, and one which was produced from a modified version of the original dataset and which excludes the record(s) relating to the individual. If the inference can only be drawn from the first version of the given data, it is clear that the inference relies on the records relating to the individual, and consequently that the given data relates to the individual."*

AFI'S COMMENTS

Paragraph 71, point (b), describes the comparison between the result obtained from the complete dataset and that obtained from the dataset without the person's records. The method is indicated without any link to techniques already in use. Without such alignment, the operator does not know which tools demonstrate the absence of specific and meaningful inferences, and the verification risks not being applied uniformly.

PROPOSED AMENDMENT

AFI proposes making explicit the relationship between the method described in paragraph 71, point (b), and in footnote 43 and the statistical confidentiality-protection techniques in use today, indicating which tools make it possible to satisfy the criterion.

§ 77 AI models

> **Guidelines 02/2026, paragraph 77**
> *"This form of inference can also be significantly more sophisticated. It may, for example, start from large sets of aggregate statistics accessible in bulk, or from data query systems. Often, this kind of inference will use multiple aggregated datasets, especially if those sets were all produced from the same original data. This is particularly true for advanced de-aggregation techniques, including attacks which can extract data*

> *from supposedly anonymous AI models. Nevertheless, a single dataset which contains a sufficiently large quantity of data may allow for the inference of information relating to a single individual, without the need for other sources."*

AFI'S COMMENTS

Paragraph 77 mentions attacks that extract data from presumably anonymous AI models. The only link to the EDPB's Opinion 28/2024 on AI models is found in footnote 45. A cross-reference in the text would ensure consistency between the two documents and would guide operators applying the No Inference criterion to models.

PROPOSED AMENDMENT

AFI proposes replacing the reference in footnote 45 with a structured reference, in the text of the Guidelines, to the EDPB's Opinion 28/2024 on AI models, in the terms indicated for paragraph 82.

§ 82 AI models and synthetic data

> **Guidelines 02/2026, paragraph 82**
> *"This kind of inference could also be drawn from data that has been aggregated to represent correlations between elements of the original information, rather than that information itself. This would, in particular, be the case for AI models or synthetic data. Specific inferences can be made by querying (or, in the case of AI models, prompting) the given data with additional information to elicit new information about a particular individual. Where such an inference is also meaningful, this would be a violation of the No Inference criterion."*

AFI'S COMMENTS

Paragraph 82 extends the No Inference criterion to data that represent correlations, in particular AI models and synthetic data, but does not indicate the verification method. The two scenarios pose different problems: for AI models, the extraction of information through queries is relevant, whereas for synthetic data it is the reproduction of training records.

Moreover, synthetic data are named only in this paragraph of the Guidelines. In the life sciences, models and synthetic data are used in study design, external control arms and the preliminary sharing of datasets. Operational guidance is also needed for the use of such data.

PROPOSED AMENDMENT

AFI proposes inserting a section dedicated to AI models and synthetic data that: (i) treats the two categories separately; (ii) clarifies whether the No Inference criterion applies to the model, to the outputs or to both; (iii) indicates the verification method; (iv) expressly refers to the EDPB's Opinion 28/2024; (v) indicates, for synthetic data, how the risk of reproducing training records is to be assessed.

3.8 Section 3.5 · Applying the criteria

§ 87 Effectiveness against a single individual

> **Guidelines 02/2026, paragraph 87**
> *"The effectiveness of a (re-) identification technique should be assessed on its ability to generate accurate results. This does not necessarily require perfect accuracy or absolute certainty; rather, the result should be at least sufficiently close, and provide at least a sufficiently high confidence in the circumstances at hand, to allow the data subjects to be distinguished and treated differently. Further, a (re-)identification technique can be successful even if it only succeeds against a single individual in a larger dataset."*

AFI'S COMMENTS

Combined with paragraph 36, the rule in paragraph 87 leads to qualifying the whole dataset as personal, even in the presence of a single re-identifiable record. Example 20, by contrast, shows that a re-identification technique is not effective if it does not make it possible to know to which individual the data relate. For large datasets, and also for datasets concerning rare disease data, a clarification reconciling the two indications is needed.

PROPOSED AMENDMENT

AFI proposes coordinating paragraph 87 and footnote 46 with the proposal formulated above for paragraph 36.

AFI also proposes referring to example 20 and clarifying that the rule whereby a re-identification technique is effective even if it succeeds against a single individual does not in itself entail the qualification of the whole dataset as personal, where the parts are treated separately.

§ 88 Safety margins

> **Guidelines 02/2026, paragraph 88**
> *"When using the contextual approach, it is important to recognise that the capabilities of different entities may vary over time. For example, a data leak could provide certain entities with access to new datasets which were previously unavailable to them. This would, in turn, allow those entities to link information with means which were, at least from that entity's perspective, previously unavailable but are now reasonably likely to be used, leading to a violation of the No Linkage criterion. To ensure the proper protection of data subjects, the EDPB therefore recommends that analyses carried out under the contextual approach should incorporate, as much as possible, adequate safety margins ensuring that the assessment remains robust as the entities' capabilities evolve."*

AFI'S COMMENTS

Paragraph 88 recommends adequate safety margins to take account of the evolving capabilities of entities, but does not define them. An undefined expression is not verifiable and does not make it possible to demonstrate that every aspect has been correctly assessed, as required by paragraph 41. A verifiable parameter also serves to demonstrate compliance.

PROPOSED AMENDMENT

AFI proposes replacing the expression "adequate safety margins" with a verifiable parameter, or setting out the criteria for determining the margins, such as the time horizon considered, the foreseeable evolution of techniques and the availability of additional information.

§ 89 Security controls

> **Guidelines 02/2026, paragraph 89**
> *"Another important consideration under the contextual approach is the accessibility of data. If data is publicly available, anybody may be able to access it with means reasonably likely to be used. If the data is subject to appropriate security controls (particularly regarding the confidentiality of the data), access to the data will constitute a mean reasonably likely to be used only for the authorised users (and not for unauthorised actors).This is relevant for both the given data itself and for any necessary additional information that might be used as part of linkage or inference."*

AFI'S COMMENTS

Paragraph 89 states that, with adequate security controls, access to the data is a means reasonably likely to be used only for authorised users and not for unauthorised entities. Example 22, by contrast, includes among the relevant entities those who breach the system despite the adoption of adequate, state-of-the-art security measures. The two indications can be read in opposite senses. A clarification would give certainty to those who must determine the security measures to adopt.

PROPOSED AMENDMENT

AFI proposes giving value to the rule in paragraph 89 and eliminating the inconsistency with example 22, clarifying under what conditions, in the presence of adequate security controls, unauthorised actors do not constitute relevant entities. If example 22 includes attackers, even only as a precaution, AFI proposes providing for this expressly and also adding an example in which adequate and verified controls exclude the relevance of such entities.

§ 90 Weight of the measures

> **Guidelines 02/2026, paragraph 90**
> *"Limits to access should be assessed holistically, taking into account the capabilities of the different entities and any contextual elements which may have a greater or lesser effect on the means they are likely to use. Technical, organisational and contractual measures can help to restrict access, but are not by themselves sufficient to make data anonymous; while controllers are encouraged to adopt these measures wherever appropriate, they should still examine the (re-)identification capabilities of anyone who might be able to access the data with means reasonably likely to be used."*

AFI'S COMMENTS

Paragraph 90 states that security measures (technical, organisational and contractual) contribute to limiting access, but are not in themselves sufficient to make the data anonymous. AFI agrees that they

cannot replace the assessment. However, the text seems to deprive security measures of autonomous weight, whereas paragraphs 29, point (b), and 89 give relevance only to effective restrictions on access.

PROPOSED AMENDMENT

Reference is made to the proposal on paragraph 34. AFI proposes recognising, in paragraph 90, specific weight for technical, organisational and contractual measures subject to independent and documented verification, without prejudice to the assessment of the re-identification capabilities of those who can access the data, thus giving coherence among the indications in the different paragraphs.

§ 91 Hashing and k-anonymity

> **Guidelines 02/2026, paragraph 91**
> *"Appropriately implemented encryption may be used to limit access to data (or, at least, limits access to a form of the data which is intelligible) and, in this way, can help to support successful anonymisation. Nevertheless, encryption is, by its very nature, intended to be reversible and differs from anonymisation. It is, therefore, important to assess if entities with access to the data could still decrypt it with means reasonably likely to be used, even if they do not currently have the decryption key (e.g. through cryptanalysis)."*

AFI'S COMMENTS

Paragraph 91 deals with encryption. The Guidelines do not mention hashing of identifiers or k-anonymity, which are among the most widely used techniques. Example 12 describes a generalisation without qualifying it as an anonymisation technique. The limits of these techniques are known: hashing preserves the one-to-one association between the person and the code, and k-anonymity applied only to quasi-identifiers does not protect when the rest of the record, such as diagnoses, prescriptions and visits collected over years, is itself distinctive. Introducing practical examples would make it possible to know when the techniques suffice and when they do not.

PROPOSED AMENDMENT

AFI proposes adding worked practical examples on hashing of identifiers and on k-anonymity, indicating the cases in which these techniques, alone or combined with other measures, make it possible to satisfy the three criteria and the cases in which they do not.

Example 22 Consistency with paragraphs 9, 30 and 89

> **Linee guida 02/2026, example 22**
> *"Example 22: The research institute described in Example 12 decides to use the contextual approach to evaluate the anonymity of the data contained in the table after deleting the original personal data.*
>
> *The research institute starts by identifying anybody who might, through means reasonably likely to be used, be able to access the table itself. The table has not been publicly released, and the research institute currently employs strong state-of-the-art cybersecurity measures, as well as other technical means to restrict unauthorised access to this dataset and prevent its members from creating any copies. Out of*

> *caution, the research institute considers that, especially over a long period of time, it is possible that the data will nevertheless leak. This could include, among other things, leaks due to human error or hacking attempts from external actors. The research institute therefore concludes that the table is accessible, through means reasonably likely to be used, by, at least: […]*
>
> *3. individuals who might hack into the system and steal and distribute the data, […]*
>
> *However, the research institution concludes that it is extremely unlikely that people who are familiar with the data subjects' personal lives would receive the data in the aftermath of a leak, which already is not very likely to occur. The same conclusion applies to all other people who would know about an individual's participation in activities that lead to the inclusion of data relating to them in the given data. Therefore, the research institution concludes that these people would not qualify as relevant entity."*

AFI'S COMMENTS

The example excludes family members and acquaintances because they would not receive the data, under the criterion of paragraph 9, with a succinct reasoning that does not refer to the chain of means of paragraph 30. The example, by contrast, includes those who breach the system, despite state-of-the-art security measures, in apparent conflict with paragraph 89.

PROPOSED AMENDMENT

AFI asks for clarification of why example 22 excludes persons close to the data subjects who could provide information to those who access the data, and for the example to be coordinated with paragraphs 9, 30 and 89.

AFI also proposes adding an example in which adequate and verified security measures exclude the relevance of entities that could breach the system.

§ 98 Singling out

> **Guidelines 02/2026, paragraph 98**
> *"If the data violates the No Record Isolation criterion, it should be checked if the isolated records allow for singling out, so that individuals are distinguished from others by matching those records with the individual's corresponding attributes. These corresponding attributes could, for example, become apparent to the relevant entity in the course of their interactions with the individual, or may be available through additional information that allows for the individual to be identified. The larger the isolated record and the more attributes it contains, the easier the singling out of the individuals becomes. If the individual can be singled out in this way, then they should be considered identifiable."*

AFI'S COMMENTS

Paragraph 98 provides for the verification of singling out only after the No Record Isolation criterion has been breached. Recital 26 and Opinion 05/2014, by contrast, treat singling out as an autonomous risk. Continuity with the previous opinion helps operators who based the assessments already carried out on the triad of singling out, linkability and inference.

PROPOSED AMENDMENT

AFI proposes explaining why singling out, indicated by Recital 26 GDPR as an example of a means, is treated as a verification following failure to satisfy the record isolation criterion, and inserting the correspondence table proposed at paragraph 28.

3.9 Concluding remark · The controller's role cannot preclude anonymisation

Cross-cutting **Role of the controller and anonymous nature of data**

AFI'S COMMENTS

The draft states that the controller's role depends on the personal nature of the data (para. 4); accepts that data may be anonymous also for the controller that anonymises them (para. 7) and that anonymisation may take place even without deletion of the originals (para. 10); and recalls, with the Wirtschaftsakademie judgment (C-210/16, footnote 7), that one may be a joint controller even without access to the data. However, it does not address the case in which data are anonymised at the controller of the original data, with tools provided by another entity that receives only the result.

This is the model of many research projects in the sector: an entity conceives and proposes the initiative to the controller of the original data (general practitioners, healthcare facilities), supplies the software that extracts and anonymises the data at source and receives only the anonymous data resulting from that flow. An interpretation is gaining ground whereby the entity that proposes the project and supplies the tool is, for that reason alone, the controller of the entire data processing from the moment of collection and, as controller, cannot consider the data it receives to be anonymous. The role of controller would derive from the proposal of the project and would in turn become the reason for denying the anonymity of those data. On this approach, anonymisation at source becomes in practice impossible for anyone promoting a project, regardless of the quality of the technique and the means available, in contrast with the relative approach that the draft itself adopts.

That outcome conflicts with the relative approach adopted by the Guidelines, which, however, do not address the case in which data are anonymised at those who produce them, with tools provided by another entity, which receives only an anonymous dataset. A position taken by the Board would ensure uniform application and legal certainty.

PROPOSED AMENDMENT

AFI proposes that the Guidelines take an express position on the relationship between the role of controller and the anonymity assessment, with a new paragraph to be inserted after paragraph 37 or in a dedicated section. The paragraph should keep two questions distinct: who is answerable for the anonymisation operation, which is a question of roles, and for whom the resulting data are anonymous, which is a question of means. AFI proposes the text below.

> **Wording proposed by AFI**
> "Even where an entity is assigned the role of controller or joint controller of the anonymisation operation, the nature of the data it receives is assessed, in accordance with paragraphs 6-7 and 11-12, on the basis of the means reasonably likely to be used from its perspective and is not inferred from its role with regard to the original data. The data received may be anonymous for that entity, in particular if it has no access to the

> source data or to additional information, if there is separation between the entities and if the anonymisation process is subject to independent verification."

AFI also proposes clarifying: (i) whether the fact of having conceived or proposed a data collection project, or of having supplied the tool with which the data are extracted and anonymised at the entity proposing the project or supplying the tool , in itself makes that entity the controller of the processing of the original personal data; (ii) whether the assessment from the controller's perspective at the time of collection, referred to in paragraph 14 and example 2, concerns only the information obligation or also the qualification of the data subsequently received; (iii) how cooperation between the entities (footnote 7) and the chain of means (footnote 21) affect the assessment where the party proposing the project has no access to the source data or to additional information. AFI also proposes illustrating the case with an example relating to anonymisation at source at physicians or healthcare facilities.

4. Bibliography

Legislation

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act).
- Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EHDS).

Case law

- Court of Justice of the EU, 5 June 2018, Case C-210/16, Wirtschaftsakademie Schleswig-Holstein.
- Court of Justice of the EU, 4 July 2023, Case C-252/21, Meta Platforms and Others v Bundeskartellamt.
- Court of Justice of the EU, 4 September 2025, Case C-413/23 P, EDPS v SRB.

Documents of the European Data Protection Board and the Article 29 Working Party

- Article 29 Working Party, Opinion 05/2014 on anonymisation techniques (WP216), adopted on 10 April 2014.
- EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, adopted on 17 December 2024.

Giorgio Bruno

President of AFI

Giorgio Cesare Maria Bruno
29/10/2026 12:03:27 UTC+0100