Let us do IT for you

Poznań, 13.10.2026 r.

Comments by DOIT BIZ Sp. z o.o. on the EDPB public consultations - Guidelines 02/2026 on Anonymisation

Subject Matter Expert Team:

Dominik Giętkowski - Team Lider

Paulina Stelmaszyk

Malwina Mikołajczak

Approved by:

Tomasz Czarnecki – CEO

Karolina Kuba - Gaździcka – Director of the DPA Department

No.	Paragraphs	Topic
A1	2.2 "Identifying the applicable perspective(s)", para. 15 (read with paras. 6–15)	Perspective of the processor (processor "inheriting" the controller's perspective)
A2	2.4.2, paras. 30–33	Threat model and rebuttal of the presumption of compliance with the law
A3	2.4.2, para. 31	Motivation versus objective incentive in the risk assessment
A4	2.4.2 "Means reasonably likely to be used", para. 34	The role of contractual measures
A5	2.4.2, para. 35 and Section 3.5.2, para. 88	Reassessment of anonymity over time
A6	2.5.2, para. 41	Documentation of the anonymisation process
A7	3.5.2, paras. 88 and 92–93	"Safety margin" and developments in AI

A1 Perspective of the processor (processor "inheriting" the controller's perspective)	
Section / paragraph	Section 2.2 "Identifying the applicable perspective(s)", para. 15 (read with paras. 6–15)
EDPB position	The Guidelines provide that whether data is personal is assessed separately from the perspective of each entity (paras. 6–7). Para. 15 constitutes an exception: where an entity processes data on behalf of a controller, the status of the data is determined by the controller's perspective - data that is personal for the controller is therefore automatically personal for the processor as well, even if the processor has no means whatsoever of identifying individuals.
Our comment	Para. 15 means that pseudonymised data transferred to a service provider acting on behalf of a controller is always personal data for that provider - even where the provider has not received the key and has no realistic possibility of establishing to whom the data relates. The status of the data is then determined by the legal form of the cooperation ("on behalf of" versus "independently" - cf. Examples 3 and 4), rather than by the actual possibility of identification. This reverses the "means reasonably likely to be used" test on which the rest of the Guidelines is based (paras. 26–33) and imposes the full GDPR regime on an entity that operates exclusively on coded data.
Justification	First, the judgment relied on in support of para. 15, C-413/23 P EDPS v SRB, only held that the information obligation (Article 15 of Regulation 2018/1725, the counterpart of Article 13 GDPR) is to be assessed from the perspective of the controller at the time of collection; the Court did not hold that the data is also personal in the hands of the recipient - on the contrary, it confirmed that pseudonymised data may not constitute personal data for an entity lacking the means of identification. Second, the rule conflicts with the definition in Article 4(8) GDPR: a processor is an entity that processes personal data - the status of the data cannot be derived from a role which itself depends on that status. Third, it gives rise to obligations that cannot be

	fulfilled (e.g. assisting with data subject rights of individuals whom the provider is unable to single out in the data - cf. Article 11 GDPR). Practical example: a bank commissions an analytics firm to produce complaint statistics and transfers only the complaint texts with codes ("customer K-1029"), while the key remains with the bank. Under para. 15, the analytics firm nevertheless processes personal data and a full data processing agreement is required. The controller thus gains nothing from careful pseudonymisation, contrary to Recital 28 and Article 25 GDPR.
Proposal	• Limit para. 15 to the proposition that follows from the judgment: the anonymity of data from the recipient's perspective does not release the controller from its own obligations. • Alternatively, allow the assessment to be made from the processor's own perspective where the controller demonstrates that the processor does not have means of identification reasonably likely to be used. **Questions to the EDPB:** • Does the rule also apply to sub-processors? • How should it be applied to a service provider acting for several controllers in parallel?

A2 Threat model and rebuttal of the presumption of compliance with the law	
Section / paragraph	Section 2.4.2, paras. 30–33
EDPB position	The threat model includes any entity receiving the data directly or indirectly, including unauthorised and malicious actors, cybercriminals and foreign intelligence agencies. Means prohibited by law are in principle not taken into account, but the presumption that the law will be followed can be rebutted where there is sufficient evidence of a concrete risk that unlawful means are nevertheless reasonably likely to be used.
Our comment	Type of issue: ambiguity and an excessive burden of proof. • Para. 33 does not indicate who bears the burden of proof. The passive wording ("can be rebutted if there is sufficient evidence"), combined with the accountability principle in Article 5(2) GDPR, will in practice shift this burden onto the controller, i.e. require it to prove a negative: that nobody will breach the prohibition. • Neither the standard of proof nor its relationship with the threshold of a likelihood that is "insignificant in reality" in para. 22 is specified. If demonstrating a "concrete risk" is easier than demonstrating that the para. 22 threshold is exceeded, para. 33 unintentionally lowers that threshold. • The list of four factors is one-directional - all of them point towards rebutting the presumption, none towards maintaining it. The absence of such counter-factors means that, once raised, a doubt becomes practically impossible to dispel. • The third factor (data "especially vulnerable to illegal access … due to a lack of protection") is not evidence of non-compliance with the prohibition but an assessment of the level of security. It introduces an Article 32 GDPR criterion into the identifiability test under Article 4(1), so that the

	same technical shortcoming is assessed twice, on two different legal bases. • Para. 30 does not provide a criterion for selecting entities for the threat model, while footnote 25 relieves the assessor from systematically considering all perspectives without indicating a selection test. Assessments carried out by different entities for comparable datasets thus cease to be comparable.
Justification	Legal argument: in Breyer (C-582/14, para. 46) and EDPS v SRB (C-413/23 P, para. 82), the CJEU applies the criterion of means reasonably likely to be used, not of conceivable or theoretically available means. It is a test of likelihood, not a test of possibility. Para. 33 as currently worded, read together with Example 8, shifts the assessment towards a test of possibility, which departs from that criterion rather than clarifying it. Para. 32 itself stresses that the presumption concerns actors "properly limited by the rule of law" - this condition should also be the point of reference when assessing its rebuttal. Practical argument: the two factual elements of Example 8 - the existence of entities outside the reach of Union law and network security that is not fully up to date - are present in almost every real-life processing configuration. In our audit practice with clients in the manufacturing, transport and e-commerce sectors, delays in updating IT components are the rule rather than the exception. If these two elements alone suffice to rebut the presumption, a finding of non-anonymity becomes the default for any organisation of average IT maturity, and para. 32 loses its normative content. Anonymisation would cease to be an available data minimisation measure, a result contrary to the role the GDPR assigns to it.
Proposal	**Drafting proposals:** • Add a sentence to para. 33 specifying that evidence of a concrete risk must relate to an identified entity or category of entities and to a specific dataset, and that a general statement on the existence of cybercrime or of entities beyond the reach of Union law does not constitute such evidence. • Add to para. 33 a second, symmetrical list of circumstances supporting the presumption (e.g. effective and enforced supervision of the entity, no history of breaches in comparable situations, verifiable safeguards commensurate with the state of the art). • Move the third factor from para. 33 to the assessment of contextual factors in para. 29, where it methodologically belongs, leaving in para. 33 only the factors relating to actual compliance with the prohibition. • Add to para. 30 a proportionality criterion for selecting entities: the model should include entities for which a concrete, documented path of access to the data or to additional information can be identified; state explicitly that foreign intelligence agencies and cybercriminals are to be considered where justified by the nature of the data, its value or the channel through which it is made available. **Questions to the EDPB:** • Is "sufficient evidence" in para. 33 to be assessed according to a standard analogous to Article 32 GDPR (state of the art, cost of implementation, nature of the risk), or independently of it?

	• How does para. 33 relate to the threshold of a likelihood that is "insignificant in reality" in para. 22 - is it the same threshold or a lower one?

A3 Motivation versus objective incentive in the risk assessment	
Section / paragraph	Section 2.4.2, para. 31
EDPB position	The EDPB cautions against using "lack of motivation" as a factor in assessing the means reasonably likely to be used, noting that motivation is difficult to demonstrate objectively, may change over time, and that an entity's actions may be inconsistent with it. At the same time, the EDPB requires the potential value of the re-identified data to the re-identifying entity, as well as the risks that re-identification entails for that entity, to be taken into account.
Our comment	Type of issue: internal inconsistency and lack of definition. • The paragraph rejects motivation as a factor and, in the same paragraph, requires the value of the re-identified data and the risk to the re-identifying entity to be assessed. Value and risk on the side of the entity are, however, an objectified measure of motivation. In substance, the Guidelines do not remove motivation from the test but replace an assessment of subjective intent with an assessment of objective incentive - without naming this shift. • The lack of terminological distinction leads to two opposite errors. First, an organisation may remove the entire question of the profitability of re-identification from its analysis, so that every technically capable entity enters the model with equal weight, regardless of whether re-identifying the dataset would have any value for it - resulting in an overestimation of risk and abandonment of anonymisation. Second, an organisation may consider the paragraph internally contradictory and disregard it, reverting to the "nobody cares" argument - perpetuating the very situation the paragraph was meant to remedy. • The Guidelines do not address anonymity assessments carried out before their adoption on the basis of a lack of interest in re-identification, nor datasets shared on the basis of such assessments. Para. 35 covers an increase in likelihood over time, but not a situation where the assessment was methodologically flawed from the outset. These are two different factual situations with different consequences for the controller's liability.
Justification	Legal argument: the criterion in Recital 26 GDPR and in the CJEU case law concerns means reasonably likely to be used. The likelihood of a means being used is a function of the entity's capability and of the incentive (cost, effort, value of the outcome and risk) on its side. Removing the incentive element from this assessment would leave only capability, turning a test of likelihood into a test of possibility. Para. 31 itself does not do this, since it requires the incentive to be considered, but its first sentence suggests otherwise - and it is this sentence that will be quoted. Practical argument: the argument of a lack of interest in re-identification has for years served as a basis for anonymity assessments and is present in

	documentation we encounter during audits - it is not a marginal phenomenon. Para. 31 undermines this basis without providing a transition path. For entities that have shared or published datasets on this basis, the absence of such guidance means continuing uncertainty as to the qualification of that data and the extent of their own liability. Comparative context: the "motivated intruder" test maintained by the UK supervisory authority (ICO) in its current anonymisation guidance makes motivation a structural parameter of the assessment, calibrated through the figure of a motivated intruder with the resources of a reasonably competent person. We do not advocate adopting this model - the figure of a single intruder poorly captures situations in which the threat arises from a combination of entities, as para. 30 rightly recognises. We note, however, that methodological divergence in the assessment of the same dataset across jurisdictions is a real cost for organisations operating in both, and a single sentence clarifying the scope of the rejection of motivation would largely remove it.
Proposal	**Drafting proposals:** • Redraft the first sentence of para. 31 so that the rejection clearly concerns intent rather than incentive - e.g.: "the assessment cannot rely on a statement or assumption that a given entity has no interest in re-identification; instead, the objective incentives should be assessed - the potential value of the re-identified data, the cost and effort of re-identification, and the risks it entails for the re-identifying entity". • Introduce in the Guidelines a conceptual distinction between "subjective motivation" (not a suitable assessment factor) and "objective incentive" (a mandatory element of the assessment), and use it consistently. • Add an example illustrating a correct assessment of incentive, in which the low value of the dataset after re-identification, the high cost of carrying it out and the high legal risk for the entity lead to the conclusion that the likelihood is insignificant - to make clear that such reasoning remains admissible. **Questions to the EDPB:** • Do anonymity assessments based on a lack of interest in re-identification carried out before the adoption of the Guidelines require revision, and does the EDPB intend to provide for a transitional period? • How should datasets shared or published on the basis of such an assessment be treated - in particular, does the "from that moment" liability rule in para. 35 apply, or does liability extend back to the time of the original assessment?

A4 The role of contractual measures	
Section / paragraph	Section 2.4.2 "Means reasonably likely to be used", para. 34
EDPB position	A prohibition set out in a contract (e.g. a prohibition on re-identification imposed on the recipient) should not be treated as a prohibition by law: contractual terms may affect the assessment of the identification risk, but should "only be used to complement technical measures" - they must be

	reliable, verifiable and enforceable, and the EDPB notes that contracts may be revised or disregarded.
Our comment	Para. 34 prejudges that contractual safeguards - whatever their quality - can never on their own lead to data being considered anonymous, and can at most supplement technical measures. This is inconsistent with para. 33, which does not grant automatic effectiveness even to statutory prohibitions but requires an examination of whether they actually work (whether they are enforced and dissuasive). Contracts are thus assessed categorically ("by definition too weak") rather than according to their actual effectiveness - even though actual effectiveness is the yardstick of the entire test.
Justification	In Breyer (C-582/14), the CJEU held that identification is excluded where it is "practically impossible" - which depends on the actual circumstances, not on the source of the prohibition. A contract between professional, supervised entities (e.g. bank–bank, hospital–research institute) with audit rights, contractual penalties and technical monitoring may reduce the likelihood of re-identification to an insignificant level; the difference compared with a statutory prohibition is one of degree, not of kind. Practical significance: a large part of data sharing - data sharing agreements, data clean rooms, clinical trials, AI consortia - relies precisely on contractual safeguards; downgrading them across the board undermines these models without offering a workable alternative.
Proposal	We propose replacing the categorical wording "should only be used to complement technical measures" with a rule of individual assessment: a contract meeting the criteria set out in para. 34 (reliable, verifiable, enforceable) should be a fully-fledged factor in the means-reasonably-likely test - by analogy with the examination of the actual effectiveness of statutory prohibitions in para. 33.

A5 Reassessment of anonymity over time	
Section / paragraph	Section 2.4.2, para. 35 and Section 3.5.2, para. 88
EDPB position	The likelihood of re-identification typically increases over time due to technological progress and the increased availability of additional information. Where it ceases to be insignificant, previously anonymous data should again be considered personal and the controller is accountable for its processing. Periodic reassessment of the likelihood of re-identification is "good practice", wherever possible and as appropriate, and analyses under the contextual approach should, as much as possible, incorporate adequate safety margins.
Our comment	Type of issue: lack of definition and internal disproportionality. • Asymmetry between consequence and obligation. The consequence of the erosion of anonymity is framed firmly (requalification of the data as personal and the controller's liability, and consequently information obligations, handling of data subject rights and assessment of whether the event constitutes a personal data breach). The only activity that allows this moment to be detected is framed in the softest possible terms: "good practice", "wherever possible", "as appropriate". The current

	wording creates an incentive not to carry out a reassessment, since its outcome can only worsen the entity's position while its omission is not sanctioned. • No reference interval. Without any point of reference, it is impossible to build a consistent internal policy or to verify its implementation in an audit; each entity will adopt a different frequency and assessments will cease to be comparable. • No list of trigger events. Para. 88 gives a single example (a data leak), and a reassessment based solely on a calendar interval will, by definition, not capture sudden events. • Safety margin without a unit of measurement. The lack of a measure and of a method for estimating the safety margin in para. 88 is developed, together with joint proposals, in comment A7. • Unclear addressee of the obligation. Para. 35 addresses reassessment to entities processing anonymised data. If the data is anonymous, the entity is not a controller within the meaning of the GDPR with respect to that dataset, so the obligation is addressed to an entity formally outside the scope of the Regulation as regards that data. For datasets passed on, it is unclear whether the reassessment is to be carried out by the anonymising entity, the recipient, or both. • No distinction between reversibly and irreversibly shared datasets. Where a dataset has been published or irreversibly shared, a reassessment has nothing to remedy, since the data cannot be withdrawn from circulation. The Guidelines treat a dataset remaining under the entity's control and a published dataset in the same way, although the risks and possible responses are entirely different.
Justification	Legal argument: para. 35 attaches full legal consequences to the erosion of anonymity, referring to case law on controller liability (C-807/21 Deutsche Wohnen, paras. 76 and 78). Since the consequence is binding, the activity that enables its detection cannot remain a mere recommendation of good practice - otherwise accountability under Article 5(2) GDPR has no object in this area. It is not necessary, however, to create a new substantive obligation: it suffices to state that reassessment forms part of demonstrating accountability for the qualification of the data where the data remains under the entity's control. Practical argument: in audits we encounter anonymisation policies as one-off documents, without any mechanism for revisiting the assessment. Introducing a reference interval together with a list of trigger events is the only solution that can be translated into an internal procedure and audited. Without it, the recommendation in para. 35 will remain a declaratory statement in documentation without operational content. Comparative context: the UK supervisory authority (ICO), in its current anonymisation guidance, recommends periodic review of anonymisation decisions, explicitly differentiating the frequency according to risk, and lists events justifying an ad hoc review (new vulnerabilities and attacks, publication of new datasets increasing linkage possibilities, changes in purposes or data combinations, the moment before granting access to a new recipient). Such a model is not at odds with the risk-based approach, as risk serves as a parameter of frequency rather than as a ground for omitting the review.

Proposal	**Drafting proposals:** • In para. 35, replace the "good practice" qualification with a statement that periodic reassessment of the likelihood of re-identification forms part of demonstrating accountability for the qualification of data as anonymous - to the extent that the data remains under the entity's control and the dataset has not been irreversibly shared. • Introduce a risk-differentiated reference interval, from which one may depart with documented justification - we propose at least every 24 months for static, low-risk datasets and at least every 12 months for datasets that are updated, include special categories of data or are shared externally. • Add an open list of events triggering an ad hoc reassessment, including at least: publication of a new, publicly available dataset that can be linked to the dataset concerned; documented progress in re-identification techniques for the relevant class of data; a personal data breach at a third party changing its linkage capabilities; an extension of the circle of recipients; a change in the purpose of processing or the combination of the dataset with another; a significant change in the security of the entity holding the dataset. • In paras. 35 and 88, distinguish datasets remaining under the entity's control from irreversibly shared datasets, stating that in the latter case a higher assessment threshold and a wider safety margin are required at the time before sharing, since a later reassessment no longer has a protective function. (For proposals on how the safety margin in para. 88 itself should be expressed and estimated, see comment A7.) **Questions to the EDPB:** • Who is the addressee of the reassessment obligation in the case of a dataset passed on - the anonymising entity, the recipient, or both? • Does the EDPB intend to indicate at least an indicative reassessment frequency, or does it leave this entirely to the controller's assessment?

A6 Documentation of the anonymisation process	
Section / paragraph	Section 2.5.2, para. 41
EDPB position	Controllers should ensure adequate documentation of the anonymisation process (including testing), demonstrating both the GDPR compliance of the process and the effectiveness of the anonymisation itself, and should retain it after the completion of the process.
Our comment	Type of issue: lack of definition, covering two separate uncertainties. First, the scope of the documentation: the Guidelines do not say whether a short note confirming that anonymisation was carried out is sufficient, or whether a detailed description of the method used, test results, persons responsible for verification and risk scenarios considered is required. Second, the retention period: the Guidelines only state that the documentation must be retained "after the completion of the anonymisation process", without specifying whether this means one year, five years, the period during which the anonymised data is used, or indefinitely.

Justification	Legal argument: the documentation obligation forms part of the accountability principle (Article 5(2) GDPR), but the GDPR itself does not specify the requirements for this type of documentation - this is precisely what the EDPB Guidelines were expected to clarify, and the current wording does not. Without a clear scope and time limit, the controller cannot be certain that it complies with para. 41, which weakens its position in the event of an inspection or a security incident, when the documentation is meant to allow a swift verification of the assumptions underlying the anonymity assessment (para. 42). Practical argument: in the absence of a common standard, controllers of different sizes will adopt very different levels of detail, which hampers the comparability of practices in the market and cooperation between entities - e.g. where the recipient of an anonymised dataset wishes to assess the reliability of the anonymisation carried out by the supplier but does not know what standard of documentation to expect. It also creates a risk of excessive, disproportionate administrative burden for smaller entities, which will document more than necessary "just in case".
Proposal	We propose that the EDPB publish a minimum list of elements of the documentation of the anonymisation process (e.g. description of the method, test results, persons carrying out verification, risks considered) and clear guidance on the retention period (e.g. linked to the period during which the anonymised data is used or to the date of the next review).

A7 "Safety margin" and developments in AI	
Section / paragraph	Section 3.5.2, paras. 88 and 92–93
EDPB position	The capabilities of entities assessed under the contextual approach may change over time; the EDPB therefore recommends incorporating "safety margins" in the anonymity assessment (para. 88). Re-identification techniques are becoming increasingly accessible, and developments in AI, in particular agentic AI, further reduce the time and cost of such attempts and facilitate combining scattered information about an individual (paras. 92–93).
Our comment	Type of issue: lack of definition, giving rise to two separate practical difficulties. First, the Guidelines require a "safety margin" to be applied but do not say how it is to be measured at all - there is no unit, no formula, not even an example of an estimation method. Second, it is unclear whether the margin is to be uniform for all types of data or should vary depending on their sensitivity (e.g. health data versus transactional data) or on the pace of development of re-identification techniques in a given field. As a result, each controller must decide for itself whether the margin adopted is "adequate", which, in the absence of any point of reference, is a largely discretionary assessment.
Justification	Legal argument: the accountability principle (Article 5(2) GDPR) requires the controller to be able to demonstrate compliance, including the soundness of the anonymisation method adopted. Without an external yardstick for the "safety margin", the controller has no way of demonstrating to the supervisory authority that its "anonymous data" assessment was reasonable

	rather than arbitrary, which makes the assessment difficult to defend in an inspection. Practical argument: given the rapid development of AI (including agentic AI referred to in para. 92), an assessment that is valid today may become outdated within months, and without quantitative or qualitative guidance every organisation, regardless of size and resources, must carry out its own, subjective analysis of the re-identification risk. This increases compliance costs and legal uncertainty, especially for smaller controllers without risk analysis functions. It also leads to divergent practices among controllers, which runs counter to the very aim of the Guidelines - a harmonised approach across the EEA.
Proposal	We propose that the EDPB: • indicate whether the margin should be proportionate to the sensitivity of the data (e.g. larger for health data); • consider a requirement of periodic verification of "anonymous" status instead of (or in addition to) a one-off margin - precisely in view of AI developments (see also comment A5 on para. 35); • provide an example of how the margin can be estimated; • clarify in para. 88 that the safety margin should be expressed in a verifiable manner - e.g. by carrying out the assessment on the assumption that the entity has access to an additional dataset which it does not hold today but which is publicly available or whose publication is foreseeable - and state that the choice of such an assumption and its justification must be documented.