CHAMBER OF DIGITAL ECONOMY

Izba Gospodarki Elektronicznej (the Chamber of Digital Economy) feedback on Guidelines 02/2026 on Anonymisation ("Guidelines")

The Chamber of Digital Economy has the privilege of uniting entrepreneurs operating in Poland in the e-commerce industry. Anonymisation is fundamental for that industry: it is the principal lawful route by which transactional, basket, logistics, fraud-prevention and audience-measurement data can be analysed, shared with partners and used to train analytical models without engaging the GDPR. The notion of anonymous data therefore does not operate at the margins of the GDPR — it determines whether large categories of ordinary commercial analytics remain feasible in the EU. For this reason, the Chamber of Digital Economy would like to submit the following comments on the proposed guidelines.

Overarching Feedback

The legal standard for anonymisation under Recital 26 GDPR is relative, risk-based and evidence-based: account is to be taken of all objective factors, including time, cost and technology, and means may be disregarded where the likelihood of identification appears in reality to be insignificant. The proposed Guidelines restate that standard correctly in the abstract. In its application, however, the Chamber is concerned that at several points of the proposed Guidelines come close to treating any residual risk as decisive. Several features of the drafted Guidelines contribute to that effect. First, the Guidelines attribute to every recipient, not only in its own means, but any means it could procure from a third party, without requiring evidence that such procurement is realistic. Second, they treat the presence of any unique combination of attribute values as a failure of the No Record Isolation criterion, a threshold which few record-level commercial datasets of realistic dimensionality could meet. Taken together, these features make it difficult to see how a controller could demonstrate that anonymisation has succeeded. That would be hard to reconcile with Recital 26 of the GDPR, which expressly contemplates that personal data may cease to be personal.

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

The Chamber of Digital Economy would also draw attention to the balance of the illustrative material. The examples are drawn predominantly from the public, healthcare, research and media sectors, and the single example addressing e-commerce presents that sector in its least favourable configuration, namely a controller-processor relationship in which the data remain personal for both parties. Research institutions are therefore given detailed reassurance which is not extended to retailers, even though the commercial sharing of fragmentary transactional data is among the most common anonymisation use cases in practice. Finally, and by contrast with Opinion 05/2014, which examined named techniques together with their respective strengths and weaknesses, the Guidelines do not assess the techniques actually available to controllers. The result is guidance which explains in detail how anonymisation may fail, but offers limited assistance on how it may be achieved. We would therefore invite the EDPB to restate the reasonable-means test as a test of realistic likelihood supported by evidence, and to supplement the Guidelines with worked examples and an annex addressing techniques.

Individual Feedback

Key statement within the Guidelines	**Input to be included when answering the public consultation**
Identifying the applicable perspective(s)	
"Example 3: An e-commerce retailer transmits excerpts from its customer records to a third-party agency for analysis. […] the retailer is able to identify the customers from those records and the information should therefore be treated as personal data for both the retailer (as the	**Issue** The only example in the Guidelines addressing the e-commerce sector presents it exclusively in the configuration in which anonymisation fails. Example 3 describes a retailer transmitting excerpts of customer records to an agency acting on its behalf and concludes that the data are personal for both parties. The immediately following Example 4 applies the contrasting treatment - assessment from the recipient's own perspective - to a hospital transmitting excerpts of patient records to an independent research institute. The favourable application of the relativity principle is therefore illustrated for the research sector alone. No example addresses the considerably more common commercial scenario in

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
controller) and the agency (as the processor).” (p. 8, Example 3)	which a retailer discloses fragmentary data, such as till-receipt or basket data stripped of all customer, payment, loyalty, device and delivery identifiers, to an independent recipient which determines its own purposes and means, never receives the source records, and has no realistic means of obtaining the additional information required to attribute those data to an individual. **Problem** The omission is material. Example 3 is capable of being read, and in our experience of national practice will be read, as establishing that a retailer's disclosure of excerpts of customer records amounts to a disclosure of personal data as a matter of course. In the Chamber of Digital Economy opinion, the relativity principle is not enough illustrated in the Guidelines for commercial scenario disclosures. **Postulate** We propose that the Guidelines include a further example in which an e-commerce retailer discloses fragmentary transactional data to an independent recipient determining its own purposes and means, and in which the EDPB concludes that the information is anonymous from the recipient’s perspective where that recipient has no means reasonably likely to be used to attribute the data to an individual. In the alternative, we would ask that Example 3 state expressly that its outcome follows solely from the processor relationship and is without prejudice to the assessment of disclosures to independent recipients.
Means reasonably likely to be used	
“Example 7: A controller wants to share certain information with its business partner. […] The controller knows that their business partner would not itself be	**Issue** Example 7 sits uneasily with the objective which the Guidelines pursue. The example attributes to a recipient a technique which that recipient cannot itself perform, on the sole basis that it “could easily hire a third party to do it”. No further element is required: the example does not refer to evidence of a market for

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
able to perform this re-identification technique. However, they could easily hire a third party to do it. That technique therefore still qualifies as a means reasonably likely to be used by the business partner." (p. 11, Example 7)	the service, to its likely cost, to the recipient's motivation, to any contractual or legal impediment, or to the risk that re-identification would create for the recipient. The conclusion therefore rests on capability considered in the abstract. **Problem** Specialist re-identification expertise can, in principle, be procured by any entity in respect of any dataset. If the theoretical availability of a contractor were sufficient to render a technique "reasonably likely to be used", every technique documented anywhere would be imputed to every recipient, and the reasonable-means test would cease to distinguish between datasets, recipients or contexts. It would then be difficult for any controller to demonstrate successful anonymisation. The difficulty is compounded by the interaction between Example 7 and paragraph 30, which lists the entities that may be capable of identifying individuals, and paragraph 31, which cautions against relying on a lack of motivation. The combined effect is that capability is treated as unlimited, while the factors that actually prevent its realization are disregarded. **Postulate** We would suggest that Example 7 be deleted or substantially redrafted. If it is retained, the example should require the anonymising controller to identify concrete and verifiable factors indicating that the potential engagement of a third party is realistic in the given case, including the availability of the service on the market, the cost of the service compared to the value of the re-identified data to that recipient, the recipient's motivation, and the legal, contractual and reputational risks that re-identification would entail. We would also ask the Guidelines to state expressly that the theoretical possibility of engaging specialist expertise does not, without more, render a technique a means reasonably likely to be used.
Periodic reassessment of likelihood to re-identify data	

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
"the likelihood of re-identification typically increases over time […] It is, therefore, good practice for entities processing anonymised data, wherever possible and as appropriate, to periodically reassess the likelihood of re-identification." (p. 14, paragraph 35) Compare footnote 3: *"a controller that has assessed a dataset as anonymous in accordance with Opinion 05/2014 before the publication of these new guidelines is not expected to conduct a new assessment." (p. 3)*	**Issue** The two statements point in different directions, and the recommendation is addressed to the processing of data which, by definition, fall outside the scope of the Regulation. **Problem** Footnote 3 exempts existing assessments from re-examination, while paragraph 35 recommends periodic reassessment of anonymised data as good practice. Read together, the two passages leave controllers without a clear position. More fundamentally, Article 2(1) GDPR excludes anonymous data from the material scope of the GDPR, and an ongoing obligation attaching to their processing would not readily find a basis in it. In practice, recommendations of this kind tend to be treated as requirements by auditors and counterparties, yet no trigger, periodicity or evidential standard is specified. **Postulate** We would welcome confirmation that, once data have been assessed as anonymous, they fall outside the material scope of the GDPR by virtue of Article 2(1), with the consequence that periodic reassessment is a recommendation of good practice rather than an enforceable obligation. Rather than recommending reassessment in general terms, we would also suggest that the Guidelines identify concrete triggers, such as a material change in the data, a documented advance in re-identification techniques applicable to the dataset in question, or the intended release of the data to a wider group of recipients.
Legal basis	
"[…] anonymisation must have a legal basis under Article 6 GDPR, and that one of the exemptions under Article 9(2) GDPR	**Issue**

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
should apply if the dataset contains special category personal data. Legal basis and, when applicable, the relevant Article 9(2) exemption should be presumed to coincide with the legal basis and exemption of the processing preceding anonymisation …" *(p. 15, paragraph 38)* See also paragraph 39 (p. 15).	Paragraph 38 makes the availability of an exemption under Article 9(2) GDPR a condition of the anonymisation wherever "the dataset contains special category personal data". The requirement is therefore triggered by the composition of the dataset as a whole, rather than being confined to the special category data actually present within it. **Problem** In the e-commerce sector, a transactional dataset of any size will almost inevitably contain a small number of records from which special categories of data could be derived, for example, a pharmacy purchase, a dietary or religious product, or an assistive device. According to paragraph 38, the presence of those few records subjects the anonymisation of the entire dataset to the Article 9 GDPR gateway, even though the great majority of the records contain only ordinary personal data. Read together with paragraph 36 and footnote 31, which treat a dataset comprising both special category and other data as special category data in its entirety, the effect is that the most demanding legal standard applies to the whole operation by reason of a marginal proportion of its content. This issue is further complicated by the fact that Article 9(2) GDPR contains no exemption for anonymisation (at least at this very stage). Where the presumption of continuity is not engaged - and it is not engaged where anonymisation is undertaken for the distinct purpose of ceasing to process personal data altogether - there may be no exemption available for an operation whose sole purpose is to remove the data from the scope of the GDPR. Therefore, the measure that is most effective in protecting data subjects becomes the hardest to justify. This is difficult to reconcile with paragraph 39, which treats immediate anonymisation with the deletion of source data as a factor in favour of the controller, and with Recital 26 of the GDPR, which presupposes that personal data can be processed in such a way that the data subject is no longer identifiable. **Postulate**

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
	We would ask that paragraph 38 be revised to confirm that the Article 9(2) GDPR requirement attaches only to the processing of the special category data actually contained in the dataset, and not to the anonymisation of the dataset as a whole, so that the presence of a limited number of such records does not subject the entire operation to the Article 9 GDPR gateway.
Personal data breach	
"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" *(pp. 15–16, paragraph 42)* *"Relevant entities may, therefore, include anybody directly or indirectly receiving the*	**Issue** The identifiability analysis is to be conducted from the perspective of unauthorised and malicious actors, whose identity, resources, intentions and technical capabilities are by definition unknown to the anonymising controller. Paragraph 31 discourages reliance on the absence of motivation, and Example 22 proceeds on the assumption that a leak will occur notwithstanding the security measures implemented. Taken together, these requirements call for an assessment which controllers are not in a position to carry out. **Problem** The obligation cannot be fulfilled by the controllers. A controller is able to document the means available to their counterparties, their processors and their own personnel. They have no comparable means of establishing the computational resources, additional datasets or technical expertise of an unidentified intruder, nor of obtaining evidence about an actor whose defining characteristic is that it operates outside any framework in which evidence is available. Paragraph 33 requires evidence before unlawful means may be taken into account, whereas Example 22 assumes a leak without applying that threshold. Please note that, since the residual possibility of unlawful access can never be reduced to zero, a test framed in these terms may be difficult to satisfy in respect of any dataset. That would extend the data protection regime to

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
data, including unauthorised and malicious actors. […] Cybercriminals. These entities may simply break the law to gain access to data not available from a law-abiding entities' perspective." *(p. 12, paragraph 30)* See also paragraph 31 (p. 13) and Example 22 (p. 28).	data which are anonymous for every entity lawfully concerned with them, which appears to go further than Recital 26 GDPR requires, and would place a documentation burden on controllers without a corresponding benefit for data subjects. **Postulate** We would ask that paragraph 30 be focused on entities whose access is realistically foreseeable in the circumstances of the case, so that the assessment rests on matters within the controller's knowledge. We would further ask that reliance on unauthorised actors be permitted only where the evidential criteria in paragraph 33 are satisfied, and that Example 22 be revised accordingly rather than assuming a leak. Finally, we would welcome confirmation in the Guidelines that unauthorised access to anonymised data does not of itself render those data personal where it is not established that the intruder has the means reasonably likely to be used to reverse the anonymisation, and that the adequacy of protection against such access falls to be assessed under Articles 32 to 34 GDPR.
The contextual approach	
"It must be emphasised that this simplified approach is not an alternative legal standard. Instead, this approach is a way to voluntarily shift the risk from false positives to false negatives […]" (p. 17, paragraph 48)	**Issue** The Guidelines present as a matter of convenience an approach which they simultaneously acknowledge may go beyond the legal standard, and which treats as personal data which are, in law, anonymous. **Problem** Guidance of this kind shapes expectations in practice. Once the EDPB has described a "simplified approach", controllers are likely to be asked by supervisory authorities, auditors and counterparties why they did not apply it, and the voluntary character of the choice may gradually erode. Treating anonymous

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
	data as personal has substantive consequences under Articles 5, 6, 12 to 22 and 30 GDPR, and is therefore not a neutral simplification. **Postulate** We would ask that the Guidelines state expressly that the contextual approach is the approach which reflects the legal standard, and that recourse to the simplified approach is entirely optional.
The three criteria — No Record Isolation	
"The No Record Isolation criterion is met if the data does not contain a unique combination of attribute values that relate to a single individual." (p. 18, paragraph 55) *"The larger a record is, and the more attributes that it contains, the higher the likelihood that the record will be unique within the given data."* (p. 18, paragraph 56) See also Example 10 (p. 20) and paragraphs 98 to 100 (p. 30).	**Issue** As formulated, the No Record Isolation criterion would be difficult for any record-level dataset of realistic dimensionality to satisfy, since it is not met where the data contain even a single unique combination of attribute values. Paragraph 56 acknowledges that uniqueness increases with the number of attributes. On the proposed reading, most customer-related records in commercial practice would be unique for example a customer basket, a returns history, a sequence of page views or a set of product interactions will almost always contain at least one unique combination across a customer base of any size, regardless of how thoroughly identifiers have been removed and regardless of whether anyone is in a position to link that combination to an individual. **Problem** The "No Record Isolation" criterion wrongly combines uniqueness and identifiability. Uniqueness is a characteristic of a dataset, whereas identifiability describes a relationship between a dataset and an entity possessing corresponding attributes. The Guidelines itself recognise this in paragraphs 98 and 99, and in Example 24, where a unique survey record is nonetheless treated as anonymous because the attributes

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
	cannot be matched to anything accessible to the relevant entity. Our concern is one of presentation with practical consequences: in supervisory practice and commercial negotiation alike, failure of the criterion is likely to be treated as giving rise to a presumption that the data are personal, with the burden falling on the controller to displace it, notwithstanding the further analysis provided for in paragraphs 98 to 100. For the e-commerce and retail sectors the practical effect would be significant, since partners, auditors and procurement functions can be expected to require a positive result on all three criteria before permitting data sharing, and few record-level transactional datasets would be able to deliver one. **Postulate** We would ask that the criterion be reformulated so that it is satisfied unless a unique combination of attribute values can be matched, by a relevant entity through means reasonably likely to be used, to corresponding attributes known to that entity. In the alternative, we would ask that record isolation be recharacterised in the text, in the summary table at paragraph 97 and in the Executive Summary as a risk indicator triggering the further analysis under paragraphs 98 to 100, rather than as a criterion of anonymity, and that the Guidelines state expressly that failure of the criterion gives rise to no presumption that the data are personal. We would further ask that Example 24 be supplemented by a commercial example to the same effect, for instance one based on record-level transactional data.
The three criteria — No Inference	
"The No Inference criterion is met if no specific and meaningful inference can be drawn from the given data. Inferences may be based on the given data and/or on additional information, including	**Issue** The clarifications in paragraphs 69 to 71 and in Examples 13 and 14 are valuable and should be retained. Paragraph 72, however, appears to qualify them substantially.

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
information about the anonymisation process." (p. 21, paragraph 67) *"inferences which, on first review, do not appear to be specific and meaningful may still be helpful for (re-) identification and should be further analysed in conjunction with the given data."* (p. 23, paragraph 72) See also paras 80 to 82.	**Problem** We warmly welcome the confirmation that an inference drawn about a person whose data were never in the original dataset does not render the given data personal, and that generalisations about the population at large do not violate the criterion. Those findings are essential to ordinary retail analytics, demand forecasting, assortment planning and model training. Paragraph 72, however, calls for further analysis of inferences which are not specific and meaningful, on the basis that they may nonetheless assist re-identification, without identifying a limiting principle. Paragraph 82 extends the criterion to AI models and synthetic data in a single sentence. The result is that a criterion which paragraphs 69 to 71 carefully confine is reopened without clear boundaries, leaving controllers unable to determine when the analysis is complete. The reference in paragraph 67 to "information about the anonymisation process" as additional information adds to the difficulty, since it appears to count against the documentation and transparency which paragraphs 40 and 41 require. **Postulate** We would ask that paragraph 72 be confined to cases in which a concrete and identified onward inference can be described rather than merely postulated; that paragraph 82 be aligned expressly with Opinion 28/2024 and, given the significance of the subject, addressed in a dedicated section or in separate guidance rather than in a single sentence; and that paragraph 67 clarify that documentation prepared in order to comply with paragraphs 40 and 41 is not to be treated as additional information available to relevant entities where it is held confidentially.
General comment	
General observation on the structure of the Guidelines compared to Article 29	**Issue**

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl

Key statement within the Guidelines	Input to be included when answering the public consultation
Working Party Opinion 05/2014 on anonymisation techniques, which examined named techniques and their respective strengths and weaknesses.	The Guidelines replace earlier guidance on anonymisation techniques, but they do not themselves assess any specific anonymisation technique. **Problem** Opinion 05/2014 provided detailed guidance on specific anonymisation techniques, explaining both their capabilities and their limitations. The current draft of the Guidelines takes a different approach, offering a framework of criteria together with twenty-five examples, the majority of which illustrate scenarios in which anonymisation is found to be insufficient. Controllers would benefit from additional worked examples demonstrating successful anonymisation in commercial contexts, to complement the existing material on the circumstances in which it may fail. **Postulate** We would ask that the Guidelines be supplemented by an annex assessing the principal anonymisation techniques against the three criteria and indicating the circumstances in which each may be expected to satisfy them. We would also ask for the inclusion of at least two fully worked examples drawn from the e-commerce and retail sectors — for instance, the disclosure of aggregated basket statistics to a commercial partner, and the disclosure of generalised transactional records for measurement purposes.

The Chamber of Digital Economy
Łucka 18/76,
00-845 Warsaw

KRS: 0000474028
NIP: 701-039-19-22
REGON: 146832492

Phone: +48 506 577 824
biuro@eizba.pl
www.eizba.pl