American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1 – Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

14 March 2025

AmCham Romania's Proposals for EDPB's Guidelines 01/2025 on Pseudonymization

#	PARA.	CURRENT TEXT	OBSERVATIONS/PROPOSALS	COMPANY
1	17	To attribute data to a specific (identified) person means to establish that the data relate to that person. To attribute data to an identifiable person means to link the data to other information with reference to which the natural person could be identified. Such a link could be established on the basis of one or several identifiers or identifying attributes.	A more precise formulation would be: Attributing data to a specific individual means determining that the individual is either identified or identifiable based on the data available within the pseudonymization domain. Attributing data to an identifiable individual to link the data to other information with reference to which the individual could be identified. Such a link could be established on the basis of one or several identifiers or identifying attributes.	Samsung Electronics Romania SRL
2	21-22, 37-38, 42-43, 60	At multiple points, the guidelines suggest that, for pseudonymization to be effective: The "pseudonymization domain" may in some instances have to be defined as including any and all third parties that may theoretically attempt to access the pseudonymized data and additional information, even if they are not authorized to do so; and it must not be possible for any party in the pseudonymization domain to identify an individual in the pseudonymized data, taking into account all means reasonably likely to be used, including accessing information beyond that actually held by the pseudonymizing controller	The guidelines adopt an overly restrictive view of pseudonymization that confuses pseudonymization and anonymization, and ignores both the text of GDPR and established CJEU case law. Based on the draft guidelines, no parties in the pseudonymization domain should be able to obtain with reasonable efforts any additional information enabling attribution of the pseudonymized data to specific data subjects. But this reasoning suffers from a fatal flaw - it adopts an overly restrictive review of pseudonymization, confusing the concepts of pseudonymization and anonymization for the reasons described below. • If it is not possible for a party to attribute data to an identifiable individual considering all means reasonably likely to be used, then the data is anonymous, not pseudonymous, with regard to that party. • Effectively pseudonymizing data must be understood as processing data in such a way that strips the data of some information, without which it is not possible to	Meta

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1 – Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

		and parties with whom the pseudonymized data is shared.	attribute the data to a specific data subject, and which is kept separate and subject to technical and organizational measures. In other words, pseudonymizing data does not require: (i) considering any and all third parties that may theoretically attempt to access the pseudonymized data and attribute it to individuals; or (ii) considering any and all means reasonably likely to be used by parties in the pseudonymization domain - including additional information that may be accessed - to attribute the pseudonymized data to individuals. • GDPR Art. 4 and Paragraph 29 make it clear that the pseudonymization domain will not have to include any and all third parties that may theoretically attempt to access the data. • GDPR Art. 4 defines "pseudonymization" as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." This definition implies two important things: (i) the "additional information" at issue is additional information - such as pseudonyms - generated by the pseudonymizing controller from an act of processing personal data; and (ii) it is exactly "such" additional information - not any other additional information - that must render an individual identifiable if combined with pseudonymized data. This, in turn, means that the pseudonymization domain cannot extend beyond the controller and parties with whom they have shared pseudonymized data; any such additional parties would not be able to attribute the pseudonymized data to specific individuals using the additional information at issue. • Paragraph 29 also underscores that the pseudonymization domain should not be understood as potentially including any and all third parties that may attempt to access the data. In particular, Paragraph 29 states that, for the purpose of incentivizing pseudonymization, pseudonymization "should be possible within the same controller." If the pseudonymization domain often required consideration of any and all third parties that may attempt to access the data, then pseudonymization often would not be possible within the same controller.	

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1 – Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			• GDPR Paragraph 26 makes clear that pseudonymization cannot require a consideration of all means reasonably likely to be used to re-identify an individual. That test applies to anonymization, not pseudonymization. • Paragraph 26 states that if it is not possible "to identify the natural person directly or indirectly" when considering "all the means reasonably likely to be used, either by the controller or by another person," then an individual is not identifiable; the data is anonymous. Data can still be pseudonymous data even if it would be possible to identify an individual considering the means reasonably likely to be used. CJEU case law also makes clear that assessing whether an individual could be identified directly or indirectly, considering all means reasonably likely to be used, is a legal test for anonymization, not pseudonymization. The CJEU in *Breyer*, *Scania*, and *IAB Europe* applied that test to determine whether data was anonymous data - not to determine whether data was pseudonymous.	
3	22, 43	The guidelines seem to suggest that, when a pseudonymizing controller shares pseudonymized data with an authorized third party, that data may not be pseudonymous with respect to the authorized third party if other, unauthorized third parties may attempt to gain access to the data and re-identify individuals using means available to them, but not to the authorized third party.	The guidelines should not address anonymization or the concept of personal data, but they do, and they imply an overly restrictive view of anonymization that conflicts with EU case law. These guidelines are intended to address the concept of pseudonymization, which has a straightforward, ordinary meaning under GDPR Art. 4. But the guidelines inappropriately extend beyond pseudonymization, addressing the concepts of anonymization and personal data both directly and indirectly, partly by confusing pseudonymization and anonymization, as described above. • Not only do the guidelines seem to confuse the concepts of pseudonymization and anonymization, but they also seem to advocate for an overly broad interpretation of personal data and an overly restrictive view of when data are effectively anonymized. • Under the guidelines it follows that if the data are not pseudonymous, then it follows that the data cannot be anonymous. But in such an instance - where the authorized third party does not have reasonably available means to re-identify individuals - then the data should be properly understood as anonymous, not pseudonymous, with regard to that party.	Meta

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1 – Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			• This is clear from case law of both the CJEU and the EU General Court. In Breyer, the CJEU emphasized that if "the risk of identification appears in reality to be insignificant" because identification would "require a disproportionate effort in terms of time, cost and man-power," then the data is anonymous from the perspective of the party for which identification would be nearly impossible. • The EU General Court built on the CJEU's Breyer ruling in SRB to emphasize that the risk of identification must be assessed from the perspective of the party holding the data. The question is not whether any third parties may theoretically be able to identify an individual; it is whether the third party in possession of the data has means reasonably likely to be used by them to identify an individual without disproportionate effort. The CJEU's judgment in the appeal of SRB is expected soon, and it may provide binding authority on the issue of anonymization, which the EDPB should not attempt to preempt in guidelines on pseudonymization.	
4	77-79	The guidelines imply that a controller is subject to this obligation whenever "it holds" pseudonymized data. In particular, the guidelines state that controllers should inform data subjects "how they can obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity. In this case, the controller may need to provide the identity and the contact details of the source of the pseudonymized data or of the pseudonymizing controller." Guidelines suggest that controllers should provide data subjects with pseudonyms.	The guidelines misunderstand how pseudonymization interacts with GDPR Art. 11 We appreciate that the EDPB recognizes the data subject rights of GDPR Arts. 15-20 generally do not apply to pseudonymized data. But the guidelines contain two misunderstandings about the obligations that GDPR Art. 11 imposed on controllers. • First, the guidelines misunderstand when controllers must inform data subjects about the applicability of Art. 11(1). In particular, the guidelines imply that a controller is subject to this obligation whenever "it holds" pseudonymized data. See 77-79. But this conflicts with the plain text of Art. 11(1), which applies "[i]f the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller." This text makes clear that a controller has to be engaged in an act of "process[ing] personal data" in the first instance for the obligations under GDPR Art. 11 to apply. If a controller never processes personal data in a particular context—if, in that context, it only ever holds data not requiring identification of a data subject - Art. 11's obligations of informing data subjects do not apply.	Meta Samsung Electronics Romania SRL

American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1 – Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

			• Second, the guidelines misunderstand what information controllers must provide to data subjects under Art. 11(2) (if and when they are obligated to). In particular, the guidelines state that controllers should inform data subjects "how they can obtain the pseudonyms relating to them, and how they can be used to demonstrate their identity. In this case, the controller may need to provide the identity and the contact details of the source of the pseudonymized data or of the pseudonymizing controller." See 79. But this goes far beyond what the text of Art. 11(2) requires. Art. 11(2) states only that, "[w]here . . . the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible." In other words, if it is "possible"- not always - the controller should inform the data subject merely that it cannot identify the data subject - nothing more. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification. Further, the guidelines' suggestion that controllers should provide data subjects with pseudonyms directly conflicts with the text of Art. 11(2), which states that it is the responsibility of the data subject to "provide additional information enabling his or her identification." • Since Article 11(2) of the GDPR does not provide that the right to object (Art. 21) cannot apply, it would be useful to include some examples illustrating how it can be preserved.	

Taken together, the guidelines' infirmities might have the effect of disincentivizing privacy-preserving practices like pseudonymization and anonymization.

- While recognizing that privacy-preserving practices like pseudonymization are valuable and should be incentivized, the guidelines seem to suggest that it will be difficult in practice to prove that data are pseudonymous, let alone anonymous.
- Being able to show that data are pseudonymous or anonymous is a powerful incentive for organizations to innovate and invest. Not only do the guidelines adopt overly restrictive views of pseudonymization and anonymization, but they also contain complicated technical discussions suggesting that achieving pseudonymization will be technically challenging in practice.