

Commentary Note to the consultation on the EDPB draft Guidelines on Pseudonymisation

Date: 28 Feb 2025

1. Summary

1.1 Key points

The Industrie 4.0 Platform welcomes the EDPB consultation on its Pseudonymisation Guidelines ("**Guidelines**"), which touches upon a topic of high importance for Industrie 4.0 and the further digitalisation of the manufacturing industry, including the development of data spaces (e.g. Factory-X and Manufacturing-X as a whole).

While agreeing with many of the points, Plattform Industrie 4.0 sees a considerable need for further clarification, amendments and guidance, particularly in the following aspects:

- ▶ The Guidelines set too high a bar for pseudonymisation to be implemented in practice by industrial players, in particular by:
 - requiring controllers and processors to consider information beyond their immediate control, including publicly accessible sources; and
 - taking the view that pseudonymised data remains personal data even if additional information is not in the same hands.
- ▶ We are concerned that the line of distinction between pseudonymisation and anonymisation is blurred. This will significantly limit the use in practice of this important tool to protect individual rights. In many Industrie 4.0 scenarios (but also otherwise), controllers process personal data, if at all, only to a very limited extent and typically of a non-sensitive nature (e.g., machine operator ID). Given the low risk associated with such data, a more lenient approach to pseudonymisation would likely foster data protection and innovation while adequately addressing related risks. Ultimately, that would serve the purpose of safe-guarding the privacy protection of data subjects more than creating too high burdens for controllers and processors, which might lead them to not even consider instituting pseudonymization as a means of protection.
- ▶ We advocate an approach, whereby the requirements for pseudonymisation are flexible and proportionate depending on the level of sensitivity of the data and related risks.
- ▶ Specifically, we are concerned that the EDPB is imposing additional burdens on the pseudonymizing controller to run extensive investigations about additional information on data subjects that could be available on the Internet and social media, in order to assess the effectiveness of pseudonymisation ("to the extent such information can reasonably be expected to be available", Para. 21 of the Guidelines). We request the EDPB to introduce more practical limitations; small and mid-size enterprises will not be in a position to carry that burden and could refrain from relying on pseudonymization all along.
- ▶ We ask the EDPB to clarify to which extent the existing pseudonymisation domain can be supplemented and adapted or whether a second pseudonymisation domain is required where the pseudonymising controller wishes to transfer data to other recipients that were not originally considered as intended recipients of such data.

- ▶ We see a need to provide further, use case oriented examples that are relevant to mechanical engineering, smart factories and Industrie 4.0; we articulate a strong need to provide clear guidance on the fundamental mechanisms and issues of pseudonymised data in the field of mechanical engineering and processing machine data.
- ▶ We consider it of utmost importance to provide official guidance on acceptable and easily usable Anonymisation Techniques, in order to enable industrial users to step outside the applicability of the GDPR.

1.2 Working Group "Legal Framework" of Plattform Industrie 4.0

Plattform Industrie 4.0 is the central German network organisation for promoting digital transformation in manufacturing and production. More than 300 stakeholders from 215 organisations in politics, business, science and academia, trade unions and associations are active in the platform. As one of the largest international and national networks, Plattform Industrie 4.0 supports German companies in implementing Industrie 4.0 in practice with specific recommendations for action, offering support and access to testing environments. International partnerships emphasise the Plattform's strong role internationally.

Since its inauguration in 2015, the Working Group "Legal Framework" of the Plattform Industrie 4.0 ("Working Group Industrie 4.0") has continuously contributed to the public debate and consultations on the EU Digital Framework through its more than 70 leading experts from industrial and technology corporations, academia and private practice.

For this consultation paper, see a list of authors at the end of the paper.

2. Response to the consultation

2.1 Importance of anonymisation and pseudonymisation for Industrie 4.0 processes

In its publications, the Working Group Industrie 4.0 has repeatedly emphasized the specific data protection perspective with regard to connected and smart manufacturing processes, including the common service delivery models of condition monitoring and predictive maintenance. Typically, controllers and processors collect and process personal data in those contexts more incidentally as a "by-catch", rather than the personal data being at heart and centre of the respective business and delivery models.

For example, the provider of maintenance services to a machine in a manufacturing process may have remote access to the log-in files of the machine operator on duty, when running error verification on the machine run times. In that case, the collection and processing of the log-files which would be considered as an incidental processing of personal data (as a by-

catch), without that processing being essential for analysing the machine operations as such.

Figure 1 depicts the shopfloor set-up in the bottom layer, marked in red is where machine operation results in personal data. Next the data contributes to the virtual image of a component or a product - here shown in the middle layer.

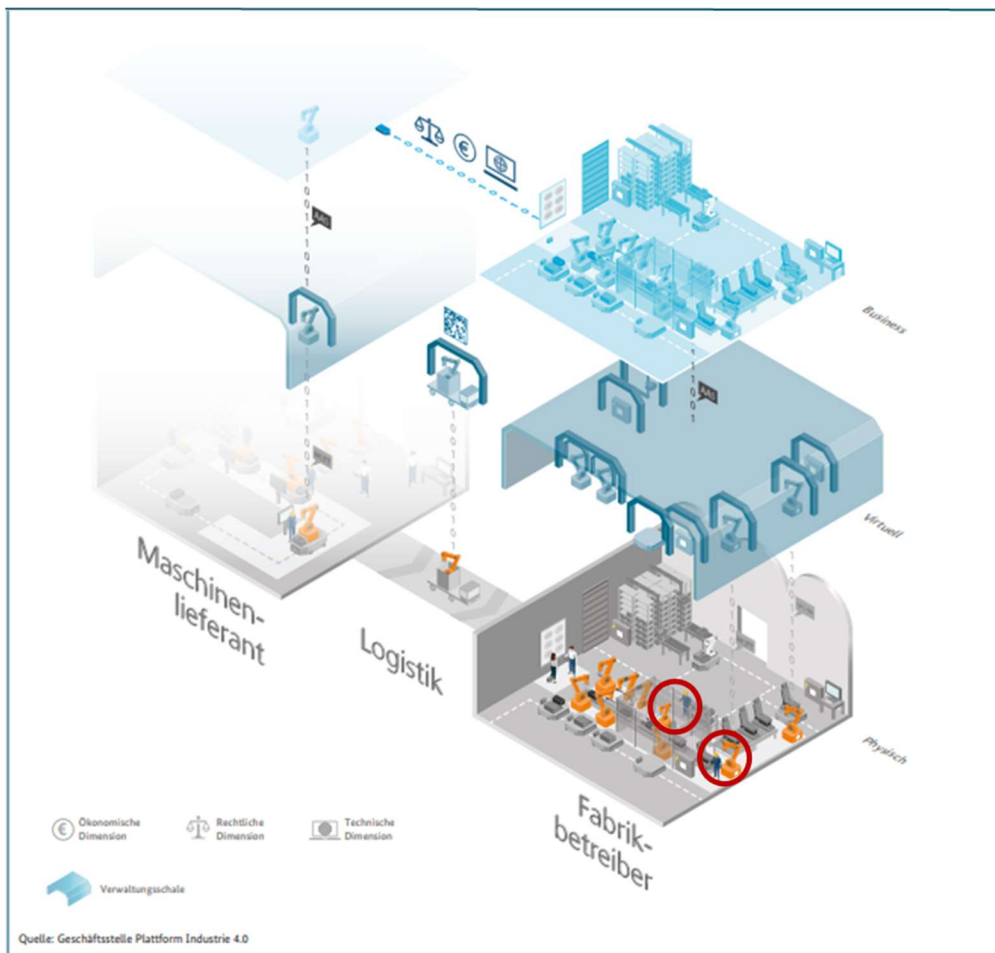


Figure 1 Plattform Industrie 4.0, Germany, Project Group Collaborative Condition Monitoring, *Der Weg zum digitalen Champion*, Plattform Industrie 4.0 - Der Weg zum digitalen Champion (accessed 2024-02)

2.2 Welcoming various parts of the Guidelines

Generally, we consider the draft Guidelines as helpful and useful guidance to industrial users. We welcome the concept of the "pseudonymisation domain", which makes it easier for the controller to define the scope of pseudonymisation and the storage and security of pseudonymised data from a technical, organisational and legal point of view.

In this context, we expressly welcome that the EDPB supplements the reference point for technical and organisational measures by the possibility for controllers and processors to

introduce (additional)) legal safeguards in the form of contractual agreements between the controllers / processors and users of pseudonymised data to protect against de-pseudonymisation.

Subject to our further comments below, we consider the pseudonymisation domain an important instrument to facilitate a more flexible handling of data and thereby increase the ability of participants within a data ecosystem (such as a data space) to exchange and transact data. We would like to accentuate in this context the need and desire to exchange data throughout data sharing arrangements in the industrial and manufacturing environment, including innovative business models based on multilateral data sharing arrangements that largely deal with non-personal data in the area of Industrie 4.0, while maintaining data protection requirements if and as required.

Further, pseudonymisation could also go a long way in helping industrial companies meet their data sharing obligations under the new EU Data Act while staying compliant with the GDPR.

2.3 Content and structure of this Commentary Note

We anticipate that the average industrial user is likely to consider the Guidelines as comprehensive rather than selective in approach. We therefore wish to articulate a considerable need to provide further differentiation, clarifications and additions. Our summary briefly addresses some key points. Against that background, we have chosen to discuss in particular the relationship to anonymisation, the pseudonymisation domain, the rights of data subjects and the technical means of pseudonymisation.

3. Anonymisation as the test case for Industrie 4.0

3.1 Call for action

Reliable anonymisation techniques are essential in the context of Industrie 4.0. Industry processes a large amount of personal data in a wide variety of processing situations. Controllers in particular from small and mid-size enterprises struggle to meet GDPR compliance obligations in full with proportionate effort (e.g., as just one example, considering the documentation requirements under Art. 30 GDPR or the procedural and documentary requirements in conducting Legitimate Interest Assessments and Data Protection Impact Assessments). The requirements to successfully pseudonymize personal data are adding an additional layer to that.

Accordingly, we note and advocate a strong interest of the industrial community to effectively anonymise any personal data before processing it within Industrie 4.0 / Manufacturing-X operations, in order to exchange production data (that may or may not have the "personal data by-catch") more freely across entity boundaries. To that end, the Working Group Industrie 4.0 urges the EDPB to provide further guidance on reliable anonymisation criteria.

In the early days of the EU Data Protection Directive, the Article 29 Working Party provided important guidance on the various methods of anonymisation in its "Opinion 05/2014 on Anonymisation Techniques" (dated 10 April 2014).¹ Notwithstanding, that this Opinion was not suited to be formally confirmed by the EDPB (inter alia, due to the lack of explicit provision on pseudonymisation in the EU Data Protection Directive), various EDPB Guidelines refer to it.² However, to date, the EDPB has not provided any clarity regarding the exact requirements for anonymisation or possible anonymisation methods.

In its draft Guidelines, the EDPB points out that controllers and processors can only achieve anonymisation by adhering to the anonymisation criteria (marg. no. 22). Notably, the EDPB does not refer to its Opinion 05/2014 nor to any other source referencing anonymisation criteria. Accordingly, we consider the current draft Guidelines as systemically incomplete, as long as the EPB has not issued a corresponding guideline on anonymisation.

We further note that the EDPB has dealt with anonymisation in its recently published "Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models", focusing hence in particular on anonymisation of personal data in the context of AI systems and training algorithms. Again, this Opinion is also unable to close the gap. While this Opinion also refers to the Opinion 05/2014 of the Article 29 Working Party, it does so explicitly and only in the context of AI models.³ In consequence, this sets an inherent limitation, and we do not see that the EDPB's statements there could be applied more generally.

3.2 Rapport between anonymisation and pseudonymisation

a) View of the EDPB

- (i) Relevance of additional information outside the immediate control of the pseudonymising controller or processor

Paragraph 21 of the Guidelines focuses on the "additional information" outside the immediate control of the pseudonymising controller or processor. The EDPB takes the view that the pseudonymising controller or processor must take such information into account when assessing the effectiveness of pseudonymisation "*to the extent such information can be reasonably expected to be available*".

This interpretation significantly widens the scope of "attribution" and therefore imposes a much stricter standard for pseudonymisation than the GDPR expressly requires. This wider scope is not inherent to the definition of "pseudonymised data" which only mentions "additional information that is kept separately and is subject to technical and organizational

¹ Art. 29 WP Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP 216.

² EDPB, Recommendations 1/2025 on the 2027 WADA World Anti-Doping Code; EDPB, Guidelines 01/2022 on data subject rights - Right of access; EDPB, Guidelines 02/2021 on virtual voice assistants; EDPB, Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications; EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default; EDPB, Guidelines 05/2020 on consent under Regulation 2016/679; EDPB, Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.

³ EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, Para. 39, 40.

measures”. This implies that the additional information must be within the immediate control of the pseudonymising controller or processor (as otherwise, no technical and organisational measures could be imposed in relation to that information). Furthermore, in Paragraphs 18 to 20 of the Guidelines, the EDPB outlines that pseudonymisation requires a process of transformation as part of which the additional information in the form of tables matching pseudonyms or cryptographic keys is generated or used. Again, this begs the question, why “additional information” is expanded beyond tables matching pseudonyms or cryptographic keys to include publicly available information such as social media posts.

Imposing this stricter standard which has the effect of requiring pseudonymising controllers or processors to search for information outside their control increases the compliance burden for companies and makes pseudonymisation an unrealistic concept in practice. This is unfortunate and unnecessary. Pseudonymisation can go a long way in protecting individuals, but only if we interpret the concept of pseudonymisation in such a way that it can realistically be implemented by small and medium sized companies across industries. Otherwise, the line between pseudonymisation and anonymisation becomes so blurred that there is no room or incentive for companies to implement pseudonymisation (see below Section 3.2 (iii)). We therefore advocate the view that information outside the pseudonymising controller or processors control would only need to be taken into account in extreme circumstances.

In addition, it is unclear what the EDPB means by “can reasonably be expected to be available”⁴. Would an industrial company or a car manufacturer be expected to search through publicly available information and test their assumption that data was successfully pseudonymised? How much effort would need to be undertaken to come to the justified conclusion that no such additional information exists? In addition, this could change anytime but it appears unreasonable to require companies to continuously monitor whether maybe somewhere outside their control, additional information might have become available jeopardising their pseudonymisation. In order to promote much needed legal certainty, once a company has come to the conclusion that it has successfully pseudonymised data, no external circumstances should change that (the same should apply to anonymisation).

(ii) Additional information in separate hands

Paragraph 22 deals with the scenario that pseudonymised data and additional information are not in the hands of the same person. Again, the scope of “attribution” is significantly expanded by the EDPB arguing that even in that case the pseudonymised data is personal if pseudonymised data and additional information could be combined having regard to the means reasonably likely to be used by the controller or by another person. The EDPB goes as far as to say that “even if all additional information retained by the pseudonymising controller has been erased, the pseudonymised data becomes anonymous only if the conditions for anonymity are met”.

In practice, it is a question of critical importance to help third parties dealing with pseudonymised data, where the third party does not hold or have access to the additional information and/or rules of attribution and, hence, cannot be considered personal data for that third party.

⁴ EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 21 sentence 3.

The EDPB now has the opportunity to provide legal certainty around this question and to take a reasonable approach. This opportunity should not be missed at a time when Europe is trying to promote and transform towards the data economy and, thereby, must accelerate in catching up with globally dominant markets. We therefore strongly suggest that:

- ▶ firstly, the EDPB does not introduce uncertain, discretionary legal terms such as “means reasonably likely to be used” without providing additional rules of interpretation at the same time; and
- ▶ secondly, the EDPB seizes the opportunity to make “pseudonymisation” a concept that can be implemented in practice without disproportionate effort through unnecessarily increasing the threshold for pseudonymisation. While the GDPR states that pseudonymised data remains personal data, we consider it preferable to exempt the third party recipient from complying with GDPR requirements where it is clear that this recipient does not have access to the additional information needed in order to attribute the data to an identified or identifiable person. We note that the ICO (see below Section b)) shares this perspective, and Advocate General Spielmann has recently endorsed this position in his opinion on the European Court of Justice (“CJEU”) Case C-413/23 P.⁵

In this context, we further note that the wording in paragraph 22 is confusing or not quite accurate”: *“If pseudonymised data and additional information could be combined having regard to the means reasonably likely to be used by the controller or by another person, then the pseudonymised data is personal.”* Pseudonymised data is always personal data. Rather, the point to make is that the pseudonymising controller or processor holding the additional information (or possibly a third-party recipient, if he has access to the same) is able to attribute such data to an identified or identifiable person.

(iii) Blurring the lines between pseudonymisation and anonymisation

Finally, the last sentence of Paragraph 22 seems to completely blur the lines between pseudonymisation and anonymisation. If all additional information needed to attribute pseudonymised data to an identified or identifiable person has been erased by a pseudonymising controller, then no attribution is possible and the threshold for anonymisation should be met. Otherwise, the pseudonymising controller would have to continuously assess the hypothesis whether any third-party person could attribute information to an identifiable person using their own or third-party information to escape the GDPR scope. We are strongly concerned that this perpetuates legal uncertainty.

b) Previous statements by national data protection authorities

(i) Qualitative thresholds for anonymisation

Until now, the European data protection authorities have applied different qualitative thresholds to establish anonymisation.

According to the CNIL's *“Guidance on pseudonymisation and anonymisation”* dated 2022 the difference between the two concepts is: *“Unlike pseudonymisation, anonymization is*

⁵ Advocate General Spielmann, Opinion in the case C-413/23 P, Para. 59.

therefore an irreversible operation." It appears that if a pseudonymising controller has erased all additional information, the pseudonymisation would not be reversible.⁶

In its "Guidance on anonymisation, pseudonymisation and privacy enhancing technologies", the ICO describes the difference between anonymization and pseudonymisation as follows: *"With pseudonymisation, the processing reduces the links between individuals and the data that relates to them but does not remove them entirely. While individuals may not be identifiable from the pseudonymous data itself, they can be identified by referring to other information held separately. Both the dataset and the additional information are therefore still personal data."*⁷ Against that statement, it appears a straight-forward conclusion that data should no longer be considered pseudonymised (= personal) data if and when the "links between the individuals and the data that relates to them" respectively the additional information is "entirely removed".

The Irish Data Protection Commission (DPC) envisions even further flexibility for achieving anonymization in its "Guidance on Anonymisation and Pseudonymisation" updated 2022: *"Therefore, to determine when data are rendered anonymous for data protection purposes, you have to examine what means and available datasets might be used to reidentify a data subject. Organisations don't have to be able to prove that it is impossible for any data subject to be identified in order for an anonymisation technique to be considered successful. Rather, if it can be shown that it is unlikely that a data subject will be identified given the circumstances of the individual case and the state of technology, the data can be considered anonymous."*⁸ The DPC provides a clear position that the controller, processor and/or third party that may receive pseudonymised data does not bear the burden of proof that it is impossible to reidentify a data subject, and that establishing a reasonable unlikelihood of re-identification suffices to achieve anonymity of the data concerned.

The EDPB now appears to be adopting stricter rules, going beyond these positions and conclusions without clear necessity from our perspective.⁹

- (ii) Taking the perspective of the controller or any other person, in order to determine effective anonymisation?

We note that data protection authorities and other bodies of the Member States take or have taken different views on whom to consider as relevant for achieving re-identification, i.e. the (pseudonymising) controller or any other third party.¹⁰ We think the former position aligns well with Rec. 26 sentence 3 GDPR: *"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."*

Accordingly, data is to be considered as personal data if any third party can determine or establish the identity of a natural person by assigning it to an identifier such as a name, an identification number, additional location data, an online identifier or one or more special

⁶ CNIL, Scientific research (excluding health): issues and advantages of anonymization and pseudonymisation, 2022.

⁷ ICO, Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, Chapter 3: Pseudonymisation, February 2022, p. 5

⁸ DPC, Guidance on Anonymisation and Pseudonymisation, June 2019, latest update April 2022; CNIL, Anonymisation of personal data, 2022, p. 5.

⁹ EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 22 sentence 4.

¹⁰ See DPC, Guidance on Anonymisation and Pseudonymisation, June 2019, latest update April 2022, p. 7; Stiftung Datenschutz, 2022, Practical Guide to Anonymising Personal Data, p. 12 et. seq.

features that express the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.

Further, we note that the Irish DPC recommends the intruder test, in order to test whether any third party – authorised or not – can identify a natural person.¹¹

For the UK, the ICO confirms that the assessment of personal data depends on the specific means available to the controller or processor to establish a personal reference:

“The status of data can change depending on who holds it. For example, pseudonymous data which you can still identify using a key or other separate identifiers might no longer be identifiable in the hands of a different organisation who does not have access to that key.

However, you cannot automatically assume that the pseudonymised data becomes anonymous information in the other party’s hands. In practice, this depends on several factors you need to assess, including:

- *the ability of the recipient to use other information to enable identification (either something in their possession, or in the public domain);*
- *the likelihood of identifiability, considering things like the cost of and time required for identification and the state of technology at the time of the processing; and*
- *the techniques and controls placed around the data once in the recipient’s hands. If you retain the pseudonymised data, it remains personal data in your hands. This is because you hold both the pseudonymised data and the additional information that allows you to identify the individuals the data relates to.”¹²*

c) Growing discrepancy between EU case law and the EDPB position

We note that the EDPB does not explicitly discuss recent CJEU case law on the definition of personal data and the identifiability of natural persons. We consider this an issue as the EDPB fails to provide clarity on its position in light of various decisions that increasingly emphasize the context and circumstances in which controllers and processors are dealing with elements of data and the attribution to natural persons. From our perspective, it is clear that the attribution of certain data to result in personal data depends on whether the controller or processor processing personal data could identify a natural person based on the information available, rather than defining as the test whether any third party could ever draw the line of connection from the information available to the identity of the data subject.¹³

Accordingly, we see a growing discrepancy between the position of the EDPB and the CJEU. The position of the EDPB is likely to increase the burden of regulatory requirements and necessary precautions imposed on controllers and processors in catering for

¹¹ DPC, Guidance on Anonymisation and Pseudonymisation, June 2019, latest update April 2022, p. 8 et. seq.

¹² ICO, Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, Chapter 3: Pseudonymisation, February 2022, p. 5.

¹³ CJEU, 19 October 2016, Breyer/Bundesrepublik Deutschland, C-582/14; CJEU, 9 November 2023, Gesamtverband Autoteile-Handel e.V./Scania, C-319/22; CJEU, 7 March 2024 IAB Europe/Gegevensbeschermingsautoriteit, C-604/22.

hypothetical scenarios that a remote third party could achieve a re-identification respectively de-pseudonymisation.

- ▶ In the *Breyer*-decision, the CJEU established a new approach by taking into account the perspective of the controller, but also considering the reasonable likelihood of the controller engaging the assistance of other persons (namely an authority or the internet service provider) in order to obtain the data subject's identity: *"Thus, it appears that the online media services provider has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority and the internet service provider, on the basis of the IP addresses stored."*¹⁴
- ▶ In its *Scania*-ruling, the CJEU has confirmed this approach by deeming the vehicle ident number ("VIN") as personal data only if the natural person who has access to the VIN has the means which reasonably allows him to identify the owner of the vehicle: *"In those circumstances, the VIN constitutes personal data, within the meaning of Article 4(1) of the GDPR, of the natural person referred to in that certificate, in so far as the person who has access to it may have means enabling him to use it to identify the owner of the vehicle to which it relates or the person who may use that vehicle on a legal basis other than that of owner."*¹⁵ When the anticipated processing implies or enables the profiling of data subjects, the CJEU considers data as personal data even if the controller cannot combine the data concerned with personal identifiers, as long as and provided that the controller is entitled to require this data through "external contributions" from third parties.¹⁶
- ▶ In a similar fashion, the European Court ("EGC") has modified in its EDPS/SRB ruling the previously known distinction between personal data and pseudonymous data when a processor (as under Art. 4 para. 8 GDPR) processes pseudonymous data on behalf of the controller.¹⁷ According to the EGC's, it should not depend on whether the processor can identify the data subject with the reasonably available assistance of another person (e.g. the controller), in order to deem the processor as processing personal data. Rather, where a processor processes data on behalf of the controller, the EGC holds that it only depends on the specific perspective and available means of the processor whether it can identify a natural person in a pseudonymised dataset: *"Therefore, since the EDPS did not investigate whether Deloitte had legal means available to it which could in practice enable it to access the additional information necessary to re-identify the authors of the comments, the EDPS could not conclude that the information transmitted to Deloitte constituted information relating to an 'identifiable natural person' (...)"*¹⁸ This reasoning is remarkable and we consider it valid and correct, in the interest of creating greater

¹⁴ CJEU, 19 October 2016 *Breyer/Bundesrepublik Deutschland*, C-582/14, Para. 48; CJEU 7 March 2024 *IAB Europe/Gegevensbeschermingsautoriteit*, C-604/22, Para. 48 et seq.

¹⁵ CJEU, 9 November 2023 *Gesamtverband Autoteile-Handel e.V./Scania*, C-319/22, Para. 48.

¹⁶ CJEU, 7 March 2024 *IAB Europe/ Gegevensbeschermingsautoriteit*, C-604/22, Para. 48 et seqq.

¹⁷ EGC, 26 April 2023 *EDPS/SRB*, T-557/20.

¹⁸ EGC, 26 April 2023 *EDPS/SRB*, T-557/20, Para. 105.

flexibility in protecting a third party recipient against "acquired" or "inherited" compliance obligations, without effectively having the control over the personal identifiers nor having the ability to achieve personal identification of the data subject concerned.

- ▶ We further note that *Advocate General Spielmann* supports the EGC's view in its opinion rendered in the appeal proceedings at the CJEU in the EDPS/SRB case T-557/20: *"In the light of those considerations, if the dispute is analysed with regard to the data as transferred to Deloitte, I am of the opinion that, contrary to what the EDPS maintains, it was necessary to determine whether the pseudonymisation of the data at issue was sufficiently robust to conclude that the complainants, who were the authors of the information transmitted to Deloitte, were not reasonably identifiable. In other words, in that context, if Deloitte had reasonable means to identify those complainants, it could be considered to be processing personal data."*¹⁹

d) Conclusion

We strongly encourage adding further clarifications to Paragraphs 22, sentences 2 and 3 of the Guideline. We also encourage a more practical approach towards pseudonymisation by setting the bar for successful pseudonymisation not quite as high as currently drafted. A more flexible approach differentiating between the sensitivity of data and the risks for data subject should also be considered (i.e. higher standards for pseudonymising health data compared to user log-ins).

We are concerned that, otherwise, achieving anonymisation could be reduced to a theoretical scenario, and at the same time leaving the controllers or processors from the industrial environment with a high degree of uncertainty whether and how they can ever reach the "safe harbour of anonymity" in practice.

We strongly recommend shifting focus in favour of the CJEU's perspective which leans towards a narrower approach, i.e. focusing on the perspective of the anonymising/pseudonymising controller.

4. Pseudonymisation Domain – a feasible solution for the German Mittelstand?

The EDPB suggests the concept of the "pseudonymisation domain" to describe the context in which pseudonymised data is processed. The pseudonymising controller must ensure by suitable technical and organizational measures that users and other third parties are not able to de-pseudonymise personal data contained in the pseudonymisation domain. Additional information that might enable identifying data subjects must be stored separately.

The construct of the pseudonymisation domain is very abstract. A visual representation of the concept would improve the general comprehension and thus also overall acceptance of this concept. It would be particularly helpful to have an example from the manufacturing

¹⁹ Advocate General Spielmann, Opinion in case C-413/23 P, Para. 59.

industry (e.g. using the predictive maintenance service model) that explains how to set up and secure the pseudonymisation domain in a practical way.

4.1 Organisational requirements

The EDPB describes the organisational requirements to conduct pseudonymisation in several places, including in Section 2.3 (Paragraph 35: risk analysis) and in Section 3.2.2 (securing the pseudonymisation domain). Although the concept of the pseudonymisation domain is explained in detail, we see a lack of concrete examples showing what the technical implementation could look like.

Further, terminology is not used consistently throughout this document: It is not sufficiently clear whether the pseudonymisation domain is to be set up and (only) controlled by the pseudonymising controller as a means of primarily enabling to create and protect pseudonymised data within the organisation of the controller, or whether the concept is intended to allow for multiple access by other parties (i.e. controllers or processors who would, however, not have access to the additional information that allows to de-pseudonymise the respective data sets). This makes the concept rather vague.

We ask the EDPB to clarify to which extent the existing pseudonymisation domain can be supplemented and adapted or whether a second pseudonymisation domain is required where the pseudonymising controller wishes to transfer data to other recipients that were not originally considered as intended recipients of such data.

4.2 Legal safeguards

In addition to technical and organisational measures, the EDPB recognises legal measures to ensure that pseudonymised data does not leave the pseudonymisation domain. The prerequisite for this is that these legal safeguards, such as contracts, can also be effectively enforced. We welcome introducing (additional) legal safeguards in the form of contractual agreements between the controllers / processors and users as this facilitates a more flexible handling of pseudonymised data and thereby increases the ability of participants within a data ecosystem (such as a data space) to exchange and transact pseudonymised data enabling the practical implementation of data spaces as part of the Commissions data strategy. However, as a next step, standard contractual clauses or further examples of adequate clauses would help to provide pseudonymising controller and processors with legal certainty.

4.3 Relevance for group structures

From our perspective, it remains an open question – requiring further clarification – what impact and benefits are of applying the pseudonymisation domain in an inter- group structure.

We advocate that establishing a pseudonymisation domain within a technically and functionally separate different organisational unit in a group of undertakings / group of

companies should allow other entities of that group who do not have access to the additional information (that would allow to de-pseudonymise data) to effectively consider the data in their hands as anonymous data, provided that the pseudonymising controller or processor has implemented all required technical, organisational and contractual safeguards that prevent such recipient entities from accessing the additional information.

For SMEs, such a separation of organisational units could be challenging in many cases as to the financial and personnel resources this requires. Smaller companies often do not have the know-how and technical means to technically separate their different organisational units. The EDPB should clarify if the implementation of the pseudonymisation domain requires the technical separation of organisational units in any case or if companies, especially smaller ones, can use this concept to document the pseudonymisation process and context.

By contrast, without further clarification, we are dubious whether controllers and processors (whether large groups, let alone small and mid-size enterprises) will make the efforts to establish pseudonymisation domains in the field of Industrie 4.0 and other industrial appliances.

5. Data subject rights and data transfers

5.1 Information obligation

Generally, the controller will need to fulfil its information obligations (Art. 13, 14 GDPR) towards data subjects, even where the data is pseudonymised.

We welcome the EDPB's clarification that the data subject rights under Art. 15 to 20 GDPR do not apply, in cases where the controller is unable to identify the data subject in accordance with Art. 11 para. 2 or Art. 12 para. 2 GDPR unless the data subject provides additional information.²⁰

Further, we understand the controller will need to inform the data subject about how they can obtain the pseudonymised data sets and to prove their identity in order to exercise their rights. Accordingly, a (third-party) controller that is processing pseudonymised data will have to refer the data subject to the pseudonymising controller. We welcome this practical approach. However, we suggest providing further guidance how the controller can demonstrate towards the data subject that *"the controller does not have (or no longer has) access to additional information allowing attribution, is demonstrably unable to lawfully obtain such information and is demonstrably unable to reverse the pseudonymisation with the assistance of another controller"*.²¹

5.2 Transferring pseudonymised data to third parties

According to the EDPB, the pseudonymising controller must check whether the risk mitigation achieved by pseudonymisation still exists if the data is transferred to a third-party

²⁰ EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 76.

²¹ EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 77.

recipient.²² Before the transfer, data controllers should check whether it is necessary to transfer the pseudonymised data including the pseudonyms. In principle, the pseudonym should not be transferred with the pseudonymised data in order to comply with the principle of data minimisation. The pseudonyms should only be transmitted with the pseudonymised data if this is necessary in order to compare data records relating to the same data subject or if the data or the result of the processing must be transmitted back to the sender.²³

According to the EDPB, the pseudonymising controller should always consider preparing a new pseudonymisation (and hence a new pseudonymisation domain) before transferring pseudonymised data in order to minimise the risk of unauthorised de-pseudonymisation.²⁴

The benefit of a second pseudonymisation domain appears questionable, should the original domain not already contain recipients of the data and possibly even unauthorised third parties? Should a new pseudonymisation domain be created for each transmission or should the existing one be supplemented or updated? This should be clarified by the EDPB. A second pseudonymisation should not be required, when – from a controller's perspective – it is highly unlikely that the third-party recipients have had or will have access to the additional information.

Furthermore, it remains questionable why a second pseudonymisation should be necessary if the EDPB requires in the following paragraph that the controller and recipient conclude contractual agreements to protect the pseudonymised data, in particular to prevent the recipient from using additional information to identify the data subjects.

5.3 Practical feasibility is questionable

Implementing pseudonymisation appears to be challenging, especially for small and mid-size enterprises. We ask the EDPB to clarify to which extent the existing pseudonymisation domain can be supplemented and adapted or whether a second pseudonymisation domain is mandatory when transferring data to other recipients that were not originally considered as intended recipients of the pseudonymised data.

5.4 Technical means and safeguards for pseudonymisation

The Guidelines provide a good general overview of the technical possibilities for pseudonymisation. We note that the technical implementations are very detailed with regard to controllers and processors operating in the pharmaceutical sector. By the same token, we see a clear lack of representation in respect of less sensitive data that is commonly used in the field of Industrie 4.0 and mechanical engineering solutions in general.

²² EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 70.

²³ EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 75.

²⁴ EDPB, Guidelines 01/2025 on Pseudonymisation, Para. 72.

Therefore, we strongly recommend providing clear guidance on the fundamental mechanisms and issues of pseudonymized data in the field of mechanical engineering, processing machine data (with personal data as a "by-catch") and Industrie 4.0 appliances.

Speaking at a technical level we note that, in general, there are other regulations regarding the pseudonymization of data, including in particular the ENISA-1 2019 and ENISA-2 2021 Reports ("**ENISA Reports**").²⁵ It would be appreciated if the EDPB could provide further clarity on the interplay and "order of precedence" between the Guidelines and the ENISA Reports.

As regards pseudonymisation methods, the EDPB mentions cryptographic algorithms and lookup tables, and refers to the Chapter 5 of the ENISA Reports for more technical details. While those explanations are helpful and appreciated, we would encourage to provide more information about the tokenization of data, which is a key aspect from a practical point of view in going forward.

In the interest of user-friendliness, we kindly suggest providing more precise citations in the references to the ENISA Reports, including page numbers would be helpful, instead of just referring to Chapters or the entire ENISA Reports (see No. 87, Footnote 22, and Footnote 25).

Further, we note that the ENISA Reports address the different classifications of risk per application. This is also somewhat addressed in the examples provided in the Appendix of the Guidelines. From a user's perspective, however, it is neither clear nor obvious how to evaluate the different assessments made under the EDPB Guidelines and the ENISA Reports.

Also, we note that EDPB puts a strong focus on use cases with considerable detail in the healthcare and pharmaceutical sector, with extensive detail on the technical implementations. By contrast, we lack use cases – in particular a typical one for small and mid-size companies – that deal with less sensitive data in the field of mechanical engineering and Industrie 4.0. For example: In many IoT applications or software platforms, the operators of such services only collect the user login information, which is obviously not comparable in terms of security levels required for processing medical data. Therefore, it would be helpful to better understand the applicable rules of pseudonymisation in the industrial sector, and the direct GDPR related benefits that a controller will have when implementing proper pseudonymisation. We think it would increase the user friendliness by adding a separate column / row in addition to "problem to be solved" that clarifies the benefit in achieving GDPR compliance through pseudonymisation.

The authors of this consultation paper include: Dr. Alexander Duisberg (Ashurst LLP), Dr. Kerstin Joos (KUKA AG), Salomé Peters (VDMA e.V.), David Plischka (Ashurst LLP), Anna von Dietze (GEA Group AG).

²⁵ For the user, there are several sources where technical terms can be explained: ENISA-1, Pseudonymisation techniques and best practices, 2019, p. 21; ENISA-2, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, p. 14; ICO, Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, Chapter 3: Pseudonymisation, February 2022, p. 15; Stiftung Datenschutz, Practice Guide and basic rules Anonymisation of Personal Data, p. 2.