ANONOS

TO: UK Domestic Data Protection Team (DCMS)
100 Parliament Street
London
SW1A 2BQ
DataReformConsultation@dcms.gov.uk

ICO Consultation on Protecting International Data Transfers
IDTA.consultation@ico.org.uk

ICO Updated Anonymisation & Pseudonymisation Guidance
anonymisation@ico.org.uk

FROM: Magali Feys[1]
Gary LaFever[2]

Anonos (www.anonos.com)

1 Fore Street Avenue
London EC2Y 9DT
United Kingdom
london@anonos.com

Rue Belliard 40
B - 1040 Brussels
Belgium
brussels@anonos.com

DATE: 11 October 2021

SUBJECT: **Embracing Heightened Standards for Anonymisation and Pseudonymisation**

We believe that embracing heightened Pan-European standards for anonymisation and pseudonymisation will enable the UK to better succeed in its goal of establishing an ambitious, pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of data to "unleash everything from new business models to informing pandemic response and helping achieve net-zero climate goals."[3] Further, the approach proposed herein enables fulfilment of Liz Denham's vision[4] that:

"Innovation is enabled, not threatened, by high data protection standards…."

through

"…recognition of the value of [the UK's] high data protection standards in international trade."

[1] Magali Feys is the Chief Strategist of Ethical Data Use at Anonos and founder of AContrario Law, a boutique law firm specialising in IP, IT, Data Protection and Cybersecurity. In addition, Magali acts as a legal advisor of the Belgian Ministry of Health where she advises on privacy matters (such as e-health network, COVID contact tracing and digital EU-COVID-certificate and the Covid Safe Ticket) and is a member of the legal working party e-Health of the Belgian Minister for Public Healthcare.
[2] Gary LaFever is the Co-Founder, Chief Executive Officer and General Counsel at Anonos, a former partner at the international law firm of Hogan Lovells and former Management Information Consultant at Accenture. Gary's 35+ years of technical and legal expertise enables him to approach data protection and utility issues from both perspectives. He is a co-inventor of 20+ granted patents with 80+ additional patent assets internationally.
[3] See *Unleashing The Power Of Data* at https://TheInnovator.news/Unleashing-the-Power-of-Data/
[4] See foreword by Elizabeth Denham, UK Information Commissioner, to the UK Department for Digital, Culture, Media & Sport consultation on "Data: a new direction" at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/10/response-to-dcms-consultation-foreword/

We respectfully submit that the information contained in this memorandum will enable the UK to better achieve its goals with respect to the:

(1) Public consultation on reforms to the UK's data protection regime ("New UK Data Direction");[5]

(2) ICO consultation on protecting international data transfers ("New UK Data Transfer");[6]

(3) ICO consultation on updating guidance on anonymisation and pseudonymisation ("New UK Guidance").[7]

We submit that these goals can be achieved by embracing the heightened standards for GDPR-compliant anonymisation and pseudonymisation as affirmed by the European Data Protection Board (EDPB)[8] and the European Commission (EC).[9]

Anonymisation

We submit that the UK approach to anonymisation should be aligned with the approach taken by EU member states.

There are two general European approaches to "anonymisation" for removing data from the scope of applicable regulation. The first approach focuses on preventing re-identification primarily in the intended recipient(s) hands - a "localised" approach. The second approach looks beyond the risk of re-identification by the intended recipient(s) to include other third parties - a more "global" approach.

The localised approach to "anonymisation" typically taken by the UK is at odds with the global approach taken by EU member states that include the risk of re-identification from third parties who, although unintended, are reasonably likely to be anticipated. It is important to note that the difference is not whether the data can be used, but whether the data is available for use without requiring the benefits of protective provisions - which would be the case if it is "anonymous" - or available for use provided it upholds the protection requirements of the EU GDPR - which would be the case if it is "pseudonymous". As anonymous data is outside the scope of the EU GDPR, organisations are free to use it without the restrictions or protections of the EU GDPR under the presumption that it poses no threat to data subjects. However, if they are wrong in that assessment, or if data is later added that leads to unauthorised re-identification, the required safeguards under the EU GDPR will not be in place.

The language of Recital 26 of the UK and the EU GDPR is identical. Recital 26 states that in determining identifiability...

> *"…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". (emphasis added)*[10]

[5] https://www.gov.uk/government/consultations/data-a-new-direction ("New UK Data Direction")
[6] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/08/ico-consults-on-data-transferred-outside-of-the-uk/ ("New UK Data Transfer")
[7] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/ ("New UK Guidance").
[8] See EDPB Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0 on 18 July 2021at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf ("EDPB Final Guidance").
[9] See EC Implementing Decision 2021/914 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on 4 June 2021 at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN ("Final EU SCCs").
[10] EU and UK GDPR Recital 26.

The statutory wording indicates that it is insufficient to evaluate identifiability from just the controller's perspective but must include other third parties "reasonably likely" to have access and the means of re-identification. **It comes down to differences in interpretation of the "reasonably likely" risk of re-identification.**

UK Perspective: Locally Anonymous Data

In the context of the proposed New UK Guidance, the ICO is proposing a "localised" approach, as indicated in its statement:

> *"In the ICO's view, the same information can be personal data to one organisation, but anonymous information in the hands of another organisation. Its status depends greatly on its circumstances, both from your perspective and in the context of its disclosure."*[11]

This localised approach to "anonymisation" is consistent with the ICO's prior position in its Code of Practice on anonymisation under the prior Data Protection Directive. Under its prior Code of Conduct, the ICO took the position that pseudonymous data should be considered anonymised when used by a researcher without access to a key needed for reidentification.[12]

The UK Health Research Authority similarly opined that pseudonymised data should not be considered personal data in the possession of someone who does not hold the re-identification key if "there is no other means to identify the individuals either by the combination of the data collected or by combining the data with other information held by, or accessible to, the staff undertaking the analysis."[13]

However, ongoing advances in data analysis techniques, hardware and the increasing availability of data sources make it increasingly straightforward to re-link data to data subjects.[14] This means that these approaches to anonymisation and pseudonymisation taken by the UK Health Research Authority and ICO are insufficient, and need to be amended, in favour of the Pan-European definitions and concepts. Research repeatedly confirms that allegedly anonymous data sets can reveal the identity of individuals when the data contains dates of birth, gender, and postal codes. Some people believe that "technology is rapidly moving towards perfect identifiability of information; datafication and advances in data analytics make everything (contain) information, and in increasingly 'smart' environments any information is likely to relate to a person in purpose or effect".[15]

Pan-European Perspective: Globally Anonymous Data

There are likely to be situations where an organisation would believe it has adequately protected data using the localised approach to anonymisation advocated by the ICO so that the data is outside the jurisdiction of the UK GDPR. However, as highlighted below, the broader global approach adopted by EU supervisory authorities would lead to a different result with respect to EU personal data under the EU GDPR. As more fully described below, if an UK organisation processes EU personal data using the localised approach to anonymisation advocated by the ICO, it may produce

[11] See page 9 at https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf
[12] Information Commissioner's Office, Anonymisation: Managing Data Protection Risk Code of Practice, Annex 1, noting that pseudonymised information would not be personal data in the hands of a researcher who lacks access to the key. See https://ico.org.uk/media/1061/anonymisation-code.pdf
[13] UK National Health Service Health Research Authority, Controllers and personal data in health and care research. See https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/
[14] See "They who must not be identified - distinguishing personal from non-personal data under the GDPR" (2020) International Data Privacy Law, 2020, Vol. 10, No. 1, at page 20 at https://academic.oup.com/idpl/article/10/1/11/5802594
[15] See "The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law" (2018) 10 Law, Innovation and Technology at page 40 at https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176

the unintended result of applying lesser protection to EU personal data than the level of protection required by EU member states.

- **Spain** (and the **European Data Protection Supervisor**)

  The Spanish Agencia Española de Protección de Datos (AEPD) and the European Data Protection Supervisor (EDPS) have issued joint guidance related to requirements for anonymity and exemption from GDPR requirements. According to the EDPS and AEPD, "anonymisation procedures must ensure that not even the data controller is capable of re-identifying the data holders in an anonymised file."[16]

- **Italy**

  The Italian Data Protection Authority (Garante) ruled against Rousseau Association (as a data processor) finding that merely removing a telephone number when other persistent unique identifiers still exist enabling indirect linking to data subject identities was inadequate protection of personal data.[17]

- **Ireland**

  The Data Protection Commission (DPC) states in its Guidance on Anonymisation and Pseudonymisation, "As set out above, data can be considered 'anonymised' from a data protection perspective when data subjects are no longer identifiable, having regard to any methods reasonably likely to be used by the data controller - or any other person to identify the data subject. Data controllers need to take full account of the latter condition when assessing the effectiveness of their anonymization technique… If the data controller retains the raw data, or any key or other information which can be used to reverse the 'anonymisation' process and to identify a data subject, identification by the data controller must still be considered possible in most cases. Therefore, the data may not be considered 'anonymised', but merely 'pseudonymised' and thus remains personal data, and should only be processed in accordance with Data Protection law."[18]

- **Denmark**

  The Danish data protection agency, Datatilsynet, found that a data controller violated the GDPR requirements for anonymisation when they retained personal information that could be later used to re-identify individuals.[19]

- **France**

  In its recommendations on the implementation of anonymisation and pseudonymisation, the Commission Nationale de l'informatique et des Libertés (CNIL) underlines that the de-identification via anonymisation must be in an irreversible manner, "Anonymisation is a treatment which consists in using a set of techniques in such a way as to make it impossible, in practice, *to identify the person by any means whatsoever and in an irreversible manner… Since the anonymisation process aims to* **eliminate any possibility of re-identification***, the future exploitation of the data is thus limited to certain types of use.*"[20]

[16] See https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf
[17] See https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974
[18] See page 7 at https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf
[19] See https://gdpr.eu/data-anonymization-taxa-4x35/
[20] See https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles

- **Germany (CJEU)**

  The *Breyer vs Germany* decision by the Court of Justice of the European Union (CJEU) is cited in the context of the New UK Data Direction as supporting the proposition that the appropriate means of identification for assessing anonymisation are those available to the relevant controller processing the data.[21] The CJEU's Breyer decision related to the German version of the prior Data Protection Directive (which was less restrictive in this regard than the original text of the Directive) and not the GDPR. There is no assurance that the CJEU would similarly rule on the appropriateness of "Local" versus "Global" requirements for compliant Anonymisation under the GDPR in light of relevant matters such as those noted above and below.

Research by data scientists at Imperial College in London and Université Catholique de Louvain in Belgium, [22] as well as a ruling by Judge Michal Agmon-Gonen of the Tel Aviv District Court,[23] highlights the shortcomings of "anonymisation" in today's Big Data world. Many believe that anonymisation reflects an outdated approach to data protection[24] that was developed when the processing of data was limited to isolated (siloed) applications prior to the popularity of Big Data processing involving the widespread sharing and combining of data. This is why the Israeli judge in the above-cited case highlights the relevance of state-of-the-art data protection principles embodied in the GDPR in her ruling that:

- *Increasing the technological capabilities that enable storing large amounts of data, known as "big data", and trading this information, enables the cross-referencing of information from different databases, and thus also trivial information such as location, may be cross-referenced with other data and reveal many details about a person, which infringe upon his privacy.*

- *Given the scope of data collection and use of information, the matters of anonymisation and reidentification have recently become important and relevant to almost every entity in Israel – both private and public – which holds a substantial amount of information.*

- *Information technologies bring new challenges and ongoing privacy vulnerabilities. One of the solutions that has been discussed in recent years is that of privacy engineering (Privacy by design), i.e., the design of technological systems in advance, to include protection of privacy.*

- *A binding rule regarding privacy engineering was established in the European Union. Regulation for the Protection of Personal Data Article 25 of the GDPR General Data Protection Regulation (which came into effect in 2018) that imposes a duty on the data controller to implement appropriate and effective technological and organizational measures both at the stage of system planning and in the stage of information processing, in other words, requiring a process of privacy engineering.*

For data to be universally "anonymous" on a global basis, we believe that the data must not be capable of being cross-referenced with other data to reveal identity. This very high standard is required because when data does satisfy these requirements, it is treated as being outside the

[21] See paragraph 123 at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf
[22] See https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html?smid=nytcore-ios-share
[23] See https://www.nevo.co.il/psika_html/minhali/MM-17-06-28857-22.htm
[24] See https://www.timesofisrael.com/data-is-up-for-grabs-under-outdated-israeli-privacy-law-think-tank-says/

scope of legal protection provided under the GDPR. Why? Because of the very "safe" and protected nature of the data that actually satisfies the stringent requirements of not being cross-referenceable or re-identifiable.

In today's world of pervasive information processing, data that a data controller holds may be readily linkable with data that is beyond the control of the controller, thereby facilitating unauthorized re-identification and exposing:

- The data controller to potential liability;
- Data sharing partners of the controller to potential liability;[25] and
- Data subjects to possible violations of their fundamental rights.

In the context of UK-EU data transfers, it is important to note that the Final EU SCCs stipulate that anonymisation "requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible."[26] In addition, the Final EDPB Guidance highlights that you must consider the availability of external data sets enabling unauthorised re-identification.[27] Therefore, relying on a localised approach to anonymisation would expose UK organisations to the unintended risk of cross-border data transfer and other violations of the EU GDPR.

Pseudonymisation

We submit that UK references to/definitions of pseudonymisation such as the following are problematic and should be modified:

- *[S]afeguards such as techniques that make it less easy to identify individuals from data sets (generically known as pseudonymisation techniques).*[28]
- *[Pseudonymisation is a] technique that replaces or removes information that identifies an individual. For example, it may involve replacing names or other identifiers (which are easily attributed to individuals) with a reference number. This is similar to how the term 'deidentified' is used in other contexts, for example the removal or masking of direct identifiers within a dataset.*[29]

The above reference and definition are *at odds with* the statutory definition of pseudonymisation in both the UK and the EU GDPR, which are now possible to satisfy using Fourth Industrial Revolution (4IR) technology.[30] The EDPB and the EC recently affirmed these definitional requirements for EU GDPR-compliant pseudonymisation in the context of the Schrems II[31] ruling by the CJEU. Relying on

[25] Under Clauses 3 and 12 of the Final EU SCCs, data controllers and processors are jointly and severally liable to data subjects, each of whom can seek redress in EU courts from any party in the data supply chain.
[26] See footnote 2 in Annex II COMMISSION IMPLEMENTING DECISION (EU) 2021/914 at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN
[27] See Paragraphs 79, 85, 86, 87 and 88 of the EDPB Final Guidance.
[28] See paragraph 35(a) at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf
[29] See page 14 at https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf
[30] See *Redesigning Data Privacy: Reimagining Notice & Consent for Human-Technology Interaction* at https://www3.weforum.org/docs/WEF_Redesigning_Data_Privacy_Report_2020.pdf and *Data Marketplaces Can transform Economies: Here's How* at https://www.weforum.org/agenda/2021/08/data-marketplaces-can-transform-economies/
[31] "Schrems II" refers to the Judgement of the Court of Justice of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18 at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en

the above problematic definitions of Pseudonymisation by the UK increases the risk of unlawful data transfers involving EU personal data by unsuspecting UK data controllers and processors.

Pseudonymisation was previously understood to generally refer to replacing direct identifiers with tokens for individual fields independently within a data set. Under the EDPB Final Guidance and the Final EU SCCs, it is clear that EU GDPR-compliant Pseudonymisation requires all of the following:

- **Protecting all data elements**: Footnotes 83 and 84 of the EDPB Final Guidance highlight that achieving GDPR Pseudonymisation status must be evaluated for a data set as a whole, not just particular fields. This requires assessing the degree of protection for all data elements in a data set, including more than direct identifiers, extending to indirect identifiers and attributes. This is underscored by the definition of “Personal Data” under GDPR Article 4(1) as more than immediately identifying information and extending to “any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

- **Protecting against singling out attacks**: Paragraph 85 of the EDPB Final Guidance mandates protection against "singling out" of a data subject in a larger group effectively making the use of either k-anonymity or aggregation mandatory.

- **Dynamism**: complying with the requirements in Paragraphs 79, 85, 86, 87 and 88 of the EDPB Final Guidance to protect against the use of information from different datasets to re-identify data subjects necessitates the use for differing purposes of different replacement tokens at different times (i.e., dynamism) to prevent re-identification by leveraging correlations among data sets without access to the “additional information held separately” by the EU data controller (see https://www.MosaicEffect.com);

- **Non-algorithmic lookup tables**: the requirement of Paragraph 89 of the EDPB Final Guidance to take into account the vulnerability of cryptographic techniques (particularly over time) to brute force attacks and quantum computing risk will necessitate the use of non-algorithmic derived look-up tables in many instances; and

- **Controlled re-linkability**: The combination of the four preceding items are necessary to meet the requirement in Paragraph 85(1) of the EDPB Final Guidance that, along with other requirements, the standard of EU GDPR pseudonymisation can be met only if “a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information.”

Pseudonymisation as affirmed in the EDPB Final Guidance and the Final EU SCCs enables organisations to conduct international data transfers according to Schrems II requirements and to lawfully process EU personal data by:

- Technologically ensuring data protection by limiting re-identification risk;

- Satisfying legitimate interests[32] requirements for minimising the risk to data subjects enabling lawful analytics, artificial intelligence (AI) and machine learning (ML) involving EU data;

- Expanding opportunities for the lawful use, sharing and combining of data; and

- Improving the accuracy of advanced analytics, AI and ML.

Furthermore, properly implemented GDPR-compliant Pseudonymisation helps to "unleash everything from new business models to informing pandemic response and helping achieve net-zero climate goals"[33] by:

- Embedding distributed trust controls[34] that travel with the data to dynamically reduce the risk of re-identification while enabling analytics, AI, ML, data sharing and combining;

- Replacing indirect identifiers and attribute information that can lead to unauthorised re-identification with dynamically assigned replacement pseudonyms that are not re-linkable, thereby introducing maximum "entropy" (uncertainty) within and between data sets to reduce the risk of r-identification; and

- Expanding the scope of processing without degrading the accuracy or relevancy of data as required by other de-identification techniques to manage re-identification risk.

International Transfer & Processing Benefits of EU GDPR-Compliant Pseudonymisation

1. **Availability of Derogations:** EU GDPR-compliant pseudonymisation – *as explicitly recognised by the EDPB and the EC* – helps to ensure lawful international transfer and processing of global data, including EU personal data, by establishing by default the processing of GDPR-compliant pseudonymised data whenever, wherever, and as often as possible (as required under GDPR Articles 25 and 32, both of which recommend pseudonymisation as a technical and organisational measure) to ensure protected

[32] Data subjects can only lawfully consent to data uses that are explicitly explained when providing consent (see GDPR Recital 32). Organisations can overcome the limitations of consent for lawful analytics, AI and ML by using distributed trust controls like GDPR-compliant Pseudonymisation to support Legitimate Interest processing (see GDPR Article 6(1)(f)) to (i) enable processing that cannot be described with required specificity at the time of initial data collection; and (ii) avoid having to seek re-consent each time different processing of data is desired. GDPR-compliant Legitimate Interest processing requires more than mere claims of having a "legitimate interest" in the outcome of processing. To serve as a valid legal basis, Legitimate Interest processing must satisfy a three-part test; the first two tests are relatively easy to meet while the third test requires technical and organisational safeguards. The three tests are: (a) Legitimate Interest test - is there a legitimate interest behind the processing; (b) Necessity test - is the desired processing necessary for that purpose; and (c) Balancing of Interest test - do technical and organisational safeguards counterbalance the interests of the data controller (or a third party) against data subjects' rights and freedoms. Technical and organisational safeguards that can "play a role in tipping the balance in favour of the controller" include functional separation and Pseudonymisation. see page 42 at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. See also https://www.Anonos.com/Legitimate-Interest

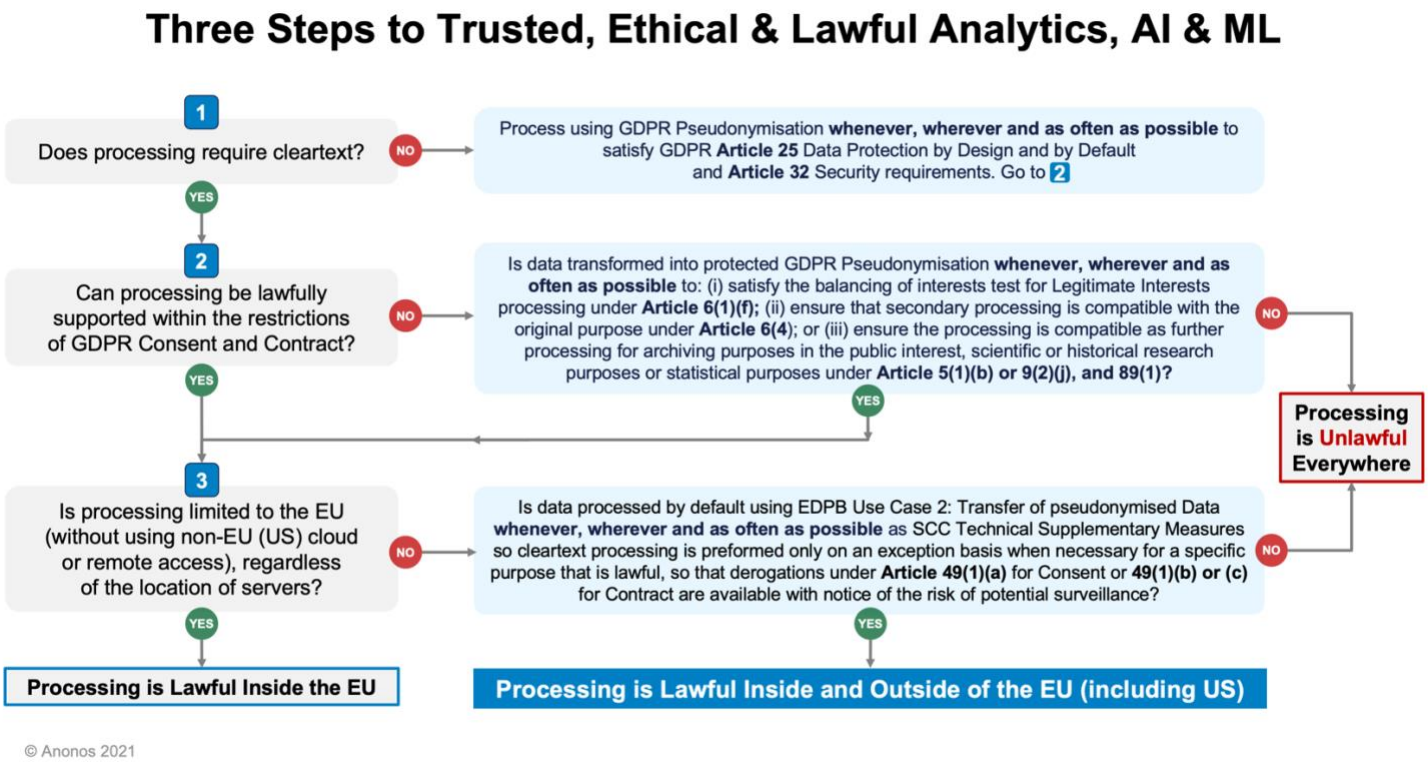
[33] See *Supra*, Note 3.

[34] The *NIST Privacy Framework: a Tool For Improving Privacy Through Enterprise Risk Management* (https://www.nist.gov/system/files/documents/2020/01/16/NIST Privacy Framework_V1.0.pdf) highlights that "trust" increases when individuals and organisations have knowledge of reliable data processing practices that manage privacy risks by increasing the predictability of processing consistent with a risk strategy to protect individuals' privacy. Technical and organisational safeguards that separate information value from identity to enforce "functional separation" embed such trust into the data which travels with the data (these safeguards are referred to as "distributed trust controls"). Functional separation enables the discovery of trends and correlations independent from applying the insights gained to the data subjects concerned. A 2015 European Data Protection Supervisor (EDPS) report (Opinion 7/2015 at https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf) highlights the potential for functional separation to "play a role in reducing the impact on the rights of individuals, while at the same time allowing organisations to take advantage of secondary uses of data." Distributed trust controls, like GDPR-compliant Pseudonymisation, enable sustainable data value by applying lawful controls that are enforceable even when the processing is decentralised.

processing within the control of the EU Data Controller (a Data Embassy[35] as it were) so that non-pseudonymised (i.e., identifying) data is processed only when necessary (helping to satisfy GDPR Articles 5(1)(b) Purpose Limitation and 5(1)(c) Data Minimisation requirements), provided that:

a. There is a legal basis to do so (e.g., based on GDPR Article 6(1)(a) consent, Article 6(1)(b) contract, Article 6(1)(f) legitimate interests (by leveraging GDPR pseudonymisation-enabled technical and organisational measures to satisfy the "balancing of interests" test[36]), Article 6(4) repurposing (which specifically recognises pseudonymisation as a safeguard to help ensure the compatibility of processing), or Article 5(1)(b) or Article 9(2)(j), together with 89(1) scientific research (which explicitly recognise pseudonymisation as a means of ensuring respect for the principle of data minimisation); and

b. The processing satisfies derogation requirements (e.g., Article 49(1)(a) based on consent, Articles 49(1)(b) or (c) based on contract), which were expanded in the EDPB Final Guidance to enable repetitive use for specific situations.[37]



[35] See Use Case 2: Transfer of pseudonymised Data, on page 31 at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf See also the Italian university dissertation on using GDPR-compliant pseudonymisation to create "Data Embassies" for purposes of Schrems II compliance available at https://www.SchremsII.com/Epilogue. Data Embassy is a trademark of Anonos.
[36] See *Supra*, Note 32.
[37] See "Expanded Flexibility for Derogations" on page 11 (internal page 2) of the consolidated university dissertation regarding Schrems II at www.Anonos.com/UniversitySchrems2Ddissertation

2. **Intra-EEA Processing Obligations:** Pseudonymisation facilitates compliance with GDPR Article 25 and 32 obligations as well as Articles 5(1)(b) Purpose Limitation, 5(1)(c) Data Minimisation, and 6(1)(f) legitimate interests processing (by leveraging pseudonymisation-enabled technical and organisational measures to satisfy the "balancing of interests" test").[38]

3. **Preference for Non-Algorithmically Derived Pseudonyms:** The use of lookup table-based pseudonyms helps to overcome the risk of brute-force unauthorised re-identification by dynamically substituting non-reversible pseudonyms for original data.[39]

   A fundamental challenge for all cryptographic data security and protection methods is that they encode the original information, so with sufficient “brute force” processing or quantum computing capabilities, data subjects are, at some level, re-identifiable from the encoded data. The unauthorised re-identification of pseudonyms within and between data sets via the “Mosaic Effect”[40] is defeated when different pseudonyms represent different occurrences of the same data for various purposes because there is no relationship among the pseudonyms without access to additional “look up” information kept separately. As a result, implementations using lookup-based EU GDPR-compliant pseudonymisation preserve individual privacy while preventing the re-identification of de-identified data, making sustainable lawful data innovation possible even in a quantum computing world.

Conclusion

In conclusion, heightened Pan-European requirements for anonymisation and pseudonymisation provide an improved structure for enhanced global data innovation and value creation by helping to transform global economies by leveraging technology. Moreover, when appropriately implemented, EU GDPR-compliant pseudonymisation not only limits re-identification risk but also expands opportunities to use, share and combine data and improve the accuracy of analytics, AI and ML. As a result, it is possible to have both state-of-the-art data protection and privacy without compromising the utility of data for innovation.[41] For the preceding reasons, we respectfully propose that the UK consider definitions of anonymisation and pseudonymisation more in line with Pan-European perspectives to increase the likelihood of a successful pro-growth and innovation-friendly data protection regime that underpins the trustworthy use of global data.

[38] See *Supra*, Note 32.
[39] See Paragraph 89 of the EDPB Final Guidance.
[40] See www.MosaicEffect.com/
[41] See *Supra*, Note 3.