ANONOS

TO: European Data Protection Board (EDPB)

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

DATE: 21 January 2022

SUBJECT: Unprotected Processing by Default vs Data Protection by Design and by Default Under the GDPR

Unprotected Processing by Default

- **Immediately Identifiable Data** – data that includes information (e.g., name, country code number, address, etc.) that immediately reveals the identity of one or more individuals.
- **Readily Reidentifiable Data** – data containing information that is not or is no longer immediately identifiable (using techniques that make it "less easy" to immediately identify an individual within a data set, such as by replacing names or other immediately identifying data with a recurring reference number or token), but for which reidentification remains easily accomplished by evaluating combinations of fields within a specific data set or through the use of readily available additional information.

Data Protection by Design and by Default

- **Practicably Protected Data** – data protected using techniques that make it impracticable to identify an individual within one or several specific data sets, without access to additional information held separately by the data controller or other authorised party (e.g., GDPR-compliant pseudonymisation).
- **Unlinkably Protected Data** – data protected using techniques that make identifying an individual within one or several specific data sets impossible (e.g., GDPR-compliant anonymisation).

I. Summary

This memorandum is submitted in response to the EDPB public consultation on Guidelines 05/2021[3] to clarify:

(i) The requirements for GDPR compliant pseudonymisation.

(ii) The benefits of pseudonymisation for Schrems II[4] and GDPR compliance.

(iii) Whether it is true that EU companies can no longer use US cloud services under any situation.[5]

Seemingly conflicting signals from different EU regulators create confusion about the obligation to implement **Data Protection by Design and by Default**[6] (e.g., per "anonymisation" and pseudonymisation" requirements under the GDPR) versus the lawfulness of "**Unprotected Processing by Default**."[7] For example, in finding that Google Analytics violates Schrems II obligations, the Austrian Data Protection Authority noted that "as long as the second respondent has the opportunity to access data in the plain text access, the [Schrems II] technical measures taken cannot be regarded as effective…" despite claims by Google that the data was "pseudonymous."[8] This even though the European Data Protection Supervisor (EDPS) recently highlighted "pseudonymisation" as the most promising supplementary measure for Schrems II compliance[9] and the EU Commission highlighted it as a key element of the adequacy for South Korea.[10]

Greater clarity and awareness of the requirements for and benefits of GDPR-compliant pseudonymisation and the obligation to pseudonymise data "as soon as possible"[11] is necessary for entities to justify changing their pervasive processing of EU personal data in the clear or readily re-linkable formats (i.e., Unprotected Processing by Default).

Absent clarity and increased awareness on these issues, data controllers and processors will continue to engage in Unprotected Processing by Default, exposing millions of data subjects to ongoing violations of their fundamental rights.[12]

EDPBmemo@anonos.com

Interactions with clients, partners, more than 6,000 participants in nearly thirty (30) webinars/presentations concerning reconciling data use and protection[13], and over 9,200 members of the LinkedIn Schrems II and Pseudonymisation group[14] reveal that Unprotected Processing by Default (as defined herein) is the most prevalent form of processing for EU personal data – *even when identity is not required* – because it is the simplest and most efficient. Also, when parties claim to enforce a specific level of protection, they usually satisfy the requirements of an inferior form of protection. For example, parties claiming to process anonymised data that falls outside of the jurisdiction of the GDPR, typically process data that is easily relinkable to identity. Similarly, parties claiming to process "pseudonymised" data usually process data that is merely "tokenised" and therefore readily relinkable to identity without requiring access to information held separately by the controller or other authorised party as required to satisfy GDPR Article 4(5) definitional requirements.

Unprotected Processing by Default (as defined herein) is a significant contributing factor to:

- **Unlawful processing involving advanced analytics and artificial intelligence (AI):**
    - Recent regulatory actions highlighting confusion regarding the requirements for establishing a lawful basis for the processing of EU personal data under the GDPR include:
        - Luxembourg's Commission Nationale pour la Protection des Données' €746/$843 million fine against Amazon;[15]
        - The Netherland's Datatilsynet's €6.5/$7.3 million fine against Grindr;[16]
        - The French Commission Nationale Informatique & Libertés' demand that Clearview cease collection and use of biometric data;[17] and
        - The Belgian Data Protection Authority's investigation into the IAB Europe's Transparency and Consent Framework.[18]
- **Noncompliant international data transfers in violation of Schrems II requirements**
    - Recent regulatory actions highlighting confusion regarding the requirements for the lawful transfer of EU personal data under Schrems II include:
        - The Austrian Data Protection Authority's decision regarding the unlawful use of Google Analytics by NetDoktor.[19]
        - The EDPS reprimand of the European Parliament for violating Schrems II requirements by using Google analytics in connection with a COVID-19 test booking site.[20]
    - EDPB clarification that Unprotected Processing by Default practices are unlawful:
        - EDPB Schrems II Recommendations Use Case 6: Transfer to Cloud Services Providers or Other Processors Which Require Access to Data in the Clear.[21]
        - EDPB Schrems II Recommendations Use Case 7: Transfer of Personal Data for Business Purposes Including by Way of Remote Access.[22]

The recent "Pseudonymous Data: Processing Personal Data While Mitigating Risks" webinar hosted by the EDPS[23] highlighted that **pseudonymisation is perhaps the most misunderstood and underutilised means to achieve simultaneous data enablement and data protection.** With it, organisations no longer need to engage in unlawful, high-risk Unprotected Processing by Default to achieve data innovation and desired business and societal outcomes. State-of-the-art pseudonymisation technology delivering 100% of the accuracy of unprotected data is available today, enabling GDPR and Schrems II compliant processing while delivering significant improvements in data processing productivity.

Table of Contents

II. Background on EDPB Public Consultation

On 18 November 2021, the EDPB adopted Guidelines 05/2021 on the Interplay Between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR ("Guidelines 05/2021"), which reference the 18 June 2021 Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data Version 2.0 ("EDPB Schrems II Recommendations")[24], and welcomed public consultation on the Guidelines 05/2021.[25] Accordingly, this memorandum is respectfully submitted to the EDPB.

On 4 June 2021, the EU Commission (the "EC") published updated Standard Contractual Clauses (SCCs) under Decision – EU 2021/914[26] (the "2021 EC SCCs"), limiting their use to transfers involving third countries not subject to the GDPR[27]. This limitation was due to the EC's view that the extraterritorial jurisdiction of the GDPR means that companies subject to the GDPR do not require a separate data transfer mechanism to ensure compliance.

This EC position is contrary to the longstanding position of the EDPB, and its predecessor, the Article 29 Working Party ("WP29"), that international transfer rules apply when transfers take place between the EU and non-EU countries, since even if the GDPR governs processing, the laws of a third country may prevent an adequate level of protection from being ensured.[28]

Data controllers and processors face considerable uncertainty since the EC does not intend the 2021 EC SCCs to be used with the supplementary measures described in the EDPB Schrems II Recommendations when a data importer is subject to the GDPR. Furthermore, commentators consider it unlikely that the EC and EDPB will agree in the near term on what supplemental SCCs should include in the case of transfers to third countries by companies subject to the GDPR.[29]

While addressed by the EDPB Schrems II Recommendations[30] and Guidelines 05/2021[31], there continues to be widespread confusion regarding the obligation to process protected versions of EU personal data. For example, consider this statement by European Data Protection Supervisor, Wojciech Wiewiórowski, during the 9 December 2021 EDPS webinar "Pseudonymous Data: Processing Personal Data While Mitigating Risks" that:

> *"The idea is that as soon as you have personal data, you should pseudonymise them if it's possible. This is the spirit of the recital 29 of the GDPR, which considers it as a basic measure, even within the same organization when utility is maintained. Not sure this is done on a regular basis. Recital 78 adds that it should be done as soon as possible."*[32]

This confusion underlies the prevalent industry-wide practice of Unprotected Processing by Default (i.e., the processing of "Immediately Identifying Data " or "Readily Reidentifiable Data," as such terms are defined herein) versus Data Protection by Design and by Default. Therefore, we respectfully request that the EDPB provide **greater clarity regarding the principles underlying the statutory requirements for pseudonymisation and the obligation to pseudonymise data "as soon as possible."**[33] This clarity is necessary for entities to justify changing their current pervasive practice of Unprotected Processing by Default.

III. Requests for EDPB Confirmation

There is widespread confusion regarding the obligation to protect EU personal data when in use during computation and analysis (i.e., the responsibility to take steps that go beyond merely using encryption to protect data when at rest and in transit so as to protect data *when in use*) **in the context of both general GDPR obligations and specific Schrems II international transfer obligations by leveraging technological controls that "travel with the data wherever it goes."**[34] For data controllers and processors to know how to satisfy legal requirements, they need greater clarity to justify allocating the resources necessary for compliance.

The current lack of clarity leads to confusion in the marketplace **whether longstanding business practices of Unprotected Processing by Default – i.e., processing data in the clear and in formats that are readily re-linkable exposing identity – must be changed for lawful processing of personal data,** both within the EEA and for purposes of compliant international data transfer.

Confusion arises due to the lack of clarity regarding when using each of the categories of information described below is lawful under the GDPR. Because the complexity and cost of processing data increases as you move from one of the below categories to the next (e.g., when moving from Category 2 – Readily Identifiable Data to Category 3 – Practicably Protected Data), **data controllers and processors resist moving from one category to the next unless there is a clear legal requirement to do so.** Even greater confusion exists regarding the requirements for and benefits of pseudonymisation under the GDPR. As a result, **Unprotected Processing by Default is the industry-wide norm for processing EU personal data, and fundamental rights of data subjects are ignored.**

For example, current proposals by the United Kingdom highlight the widespread nature of the misunderstandings regarding the requirements for GDPR-compliant anonymised (i.e., "Unlinkably Protected Data" as defined below) and pseudonymised (i.e., "Practicably Protected Data" as defined below) by advocating positions contrary to Pan-European principles:

- Requiring only "localised" protections to satisfy UK GDPR requirements for "anonymisation" versus more stringent Pan-European "globalised" protections;[35] and

- Recognising Readily Reidentifiable Data (as defined below) as complying with UK GDPR pseudonymisation requirements versus the GDPR requirement that it is not possible to identify an individual without access to additional information held separately by the data controller or other authorised party (i.e., as required to achieve Category 3 – Practicably Protected Data under the categories above).[36]

To ensure the predictability of compliant operations and the uninterrupted benefit from data analysis, artificial intelligence, (AI) machine learning (ML), sharing, combining, and enriching for clients, partners, and the more than 9,200 members of the LinkedIn Schrems II and Pseudonymisation group, we respectfully request the EDPB to confirm the following topics:

A. Pseudonymisation vs Unprotected Processing by Default

B. Heightened GDPR Requirements for Pseudonymisation

C. Benefits of GDPR-Compliant Pseudonymisation

D. Lawfulness of Combining EDPB Schrems II Recommendations and 2021 EC SCCs

III.A - Pseudonymisation vs Unprotected Processing by Default

For purposes of assessing Unprotected Processing by Default (as defined herein), information about individuals can be separated into the following four (4) categories:

Unprotected Processing by Default

1. **Immediately Identifiable Data** – data that includes information (e.g., name, country code number, address, etc.) that immediately reveals the identity of one or more individuals.

2. **Readily Reidentifiable Data** – data containing information that is not or is no longer immediately identifiable (using techniques that make it "less easy"[37] to immediately identify an individual within a data set, such as by replacing names or other immediately identifying data with a recurring reference number or token), but for which reidentification remains easily accomplished by evaluating combinations of fields within a specific data set or through the use of readily available additional information.

Data Protection by Design and by Default

3. **Practicably Protected Data** – data protected using techniques that make it impracticable to identify an individual within one or several specific data sets, without access to additional information held separately by the data controller or other authorised party (e.g., GDPR-compliant pseudonymisation).[38]

4. **Unlinkably Protected Data** – data protected using techniques that make identifying an individual within one or several specific data sets impossible (e.g., GDPR-compliant anonymisation).[39]

III.A.1 - Requested Confirmation: Documentation Requirements

We respectfully request that the EDPB confirm the obligation of data controllers and processors – *both in the context of complying with general GDPR responsibilities as well as Schrems II specific responsibilities* – to document the technical measures and mechanisms (in the context of international transfers, sometimes referred to as supplemental measures) that they implement under GDPR Articles:

- 5 - Principles Relating to Processing of Personal Data,
- 24 - Responsibility of the Controller,
- 25 - Data Protection by Design and by Default,
- 28 - Processor,
- 30 - Records of Processing Activities,
- 32 - Security of Processing,
- 34 - Communication of a Personal Data Breach to the Data Subject,
- 35 - Data Protection Impact Assessment,
- 46 - Transfers Subject to Appropriate Safeguards,
- 49 - Derogations for Specific Situations, and
- 89 - Safeguards and Derogations Relating to Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes, and otherwise.

III.A.2 - Requested Confirmation: Prohibitions on Unprotected Processing by Default within the EU

We respectfully request confirmation by the EDPB of the prohibitions on Unprotected Processing by Default (i.e., processing Immediately Identifying Data and Readily Reidentifiable Data as defined above) unless a lawful basis exists to do so, even when processing occurs solely with the EU regardless of whether an international data transfer of EU personal data is involved.[40]

III.A.3 - Requested Confirmation: Pseudonymisation for Legitimate Interests Processing

In recognition of the following statement by Thomas Zerdick, Head of Technology and Privacy at the European Data Protection Supervisor (EDPS):[41]

> "The first rule in data protection is: if you do not need personal data, do not collect personal data; and The second rule in data protection is: if you really need personal data, then start by pseudonymising this personal data;"

we respectfully request confirmation by the EDPB regarding the capabilities of GDPR-compliant pseudonymisation to enable organisations to cease reliance on unlawful high-risk Unprotected Processing by Default by enabling GDPR-compliant Legitimate Interests as a lawful basis for legally processing EU personal data to achieve data-driven outcomes.

Both historically and continuing up to the present, the legal ground of Legitimate Interests has been misused and misapplied for processing personal data to the benefit of data controllers and the detriment of data subjects. A number of key industry players and commentators, including Privacy International, Brave, and the IAB, have noted that:

> *"It is self-evident that companies cannot treat their business needs / the pursuit of their business models as synonymous with 'legitimate interests'. The mere fact that a data controller may desire to engage in intrusive profiling in order to make money off its services is not sufficient. As Recital (47) of GDPR makes clear, what is legitimate should turn at least in part on whether a legitimate interest is served due to the relationship between the controller and subject."*[42]
>
> *"The tracking industry has misused legitimate interest for years."*[43]
>
> *"We have created a messy and frightening marketplace built on the collection and use of personal information that scares the daylights out of a lot of people because they don't understand it and cannot control it. We've built it in a way that requires a doctorate in engineering to understand. Governments have rightly stepped in to attempt to offer fixes, but their laws also are difficult to comprehend, by consumers and businesses alike."*[44]

This prior and continuing improper use, however, does not foreclose the rights of current and future data controllers to avail themselves of the different legal bases available to them under the GDPR and the e-privacy Directive (and eventually the e-privacy Regulation), as applicable to their circumstances. The following quote speaks to the promise of lawful Legitimate Interests-based data innovation and protection:

> *"I personally think that after so many years of flawed cookie consent, it is a productive thing to do to introduce another approach into the legislative debate. My view is that 'legitimate interests' is misunderstood and underrated as a regulatory mechanism to protect our privacy."*[45]

While the importance of consent under the GDPR is manifest, we cannot ignore the clear requirements established for securing GDPR-compliant consent. No one wants to run the risk of (i) nullifying the protections intended for data subjects by "watering down" the requirements for compliant consent under the GDPR, including requiring that data subjects are sufficiently informed and aware of what they are agreeing to, nor the risk of (ii) removing from the global data ecosystem all societal benefits from the processing of data that is too difficult to explain at the time of collection.

The following commentary highlights this predicament:

> *"The underlying logic of data-processing operations and the purposes for which they are used have now become so complex that they can only be described by means of intricate privacy policies that are simply not comprehensible to the average citizen because of both their content and their excessive length. The*

> *result is that hardly anybody reads these privacy policies. This complexity renders individuals powerless and fosters indifference, with the result that many people simply click "OK" when using online services."*[46]
>
> *"The torrent of data being generated from and about data subjects imposes an undue cognitive burden on individual data subjects. Overwhelming them with notices is ultimately disempowering and ineffective in terms of protection — it would take the average person about 250 working hours every year, or about 30 full working days — to actually read the privacy policies of the websites they visit in a year."*[47]
>
> *"Another challenge of relying on consent is that convenience and people's limited capacity to make rational decisions prevent people from seriously spending time and intellectual effort on reading the privacy statements of every website, app, or service they use….the simpler you make the consent procedure, the less will users understand what they actually consent to; and the more meaningful you make the consent procedure (providing sufficient information about what will happen with the data), the less convenient the consent will become."*[48]
>
> *"Irrational behaviour means, in the end, that citizens do not always make a rational decision, partly due to lack of time, a short-term horizon or insufficient knowledge. The long and often complex privacy agreements that service users often agree to without reading them, are an example here."*[49]

If consent is the only basis on which EU personal information can be processed, we face a Hobson's Choice:[50]

- Uninformed consent, which is a fiction we tell each other to make everyone feel better but places all the risk on the data subject, or
- No collection or processing at all for any complex research (health, scientific, marketing or otherwise) simply due to the complexity in explaining what is happening behind the scenes.

For these reasons alone, the availability of consent as a legal basis for the complex processing of EU personal data is limited at best. It is not possible to secure GDPR-compliant consent for processing activities that occur in the future when they cannot be described with required specificity at the time of collection. Furthermore, consent to desired processing cannot be a condition for receiving a product or service – a data subject must be offered a genuine choice, or their consent is not freely given. And finally, if consent is not obtained in full compliance with GDPR requirements, "the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful."[51] Consequently, for all practical purposes, it is nearly impossible to rely on GDPR compliant consent as a lawful basis for complex data analysis, artificial intelligence, (AI) machine learning (ML), sharing, combining, and enriching.

The foregoing limitations of consent in complex processing situations is one of the reasons that Legitimate Interests exists as an alternate legal basis. The EDPB has previously noted that the Legitimate Interests legal basis[52] requires a controller to satisfy three conditions:[53]

1. **Legitimate Purpose:** the identification and qualification of a legitimate purpose pursued by the controller or by a third party. This interest of the controller or third party may be broader than the purpose of the processing but must be present at the processing date.[54]
2. **Necessity:** the need to process the personal data must be established as a requirement for the legitimate interest pursued.[55]
3. **Balancing of Interests:** the legitimate interest of the controller or third party must be balanced against the interests or fundamental rights and freedoms of the data subject, including the data subject's rights to data protection and privacy, considering the particular circumstances of the processing.[56]

If a proposed data use satisfies both the Purpose and Necessity tests, then the Balancing of Interests test must be applied to assess the impact of the intended processing on the interests or fundamental rights and freedoms of data subjects. In performing the assessment of relevant "impact", the Article 29 Working Party has stated:

> *"The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion*

> *covers any possible (potential or actual) consequences of the data processing. For the sake of clarity, we also emphasise that the concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach. Instead, the notion of impact, as used here, encompasses the various ways in which an individual may be affected - positively or negatively - by the processing of his or her personal data."*[57]

The need to assess the collective interests at stake on both sides of the balancing of interests equation – i.e., the interest of the data controller (or a third party) and the interests of the data subject – are affirmed in opinions of the EDPB (including its predecessor WP29) and decisions of the Court of Justice of the European Union ("CJEU"). Citing the CJEU rulings in Google Spain and "Schrems I", Professors Lokke Moerel and Corien Prins highlight in *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, that "the clear signal is that collective interests must also be involved in these considerations. Only then can full account be taken of the constitutional basis for personal data protection at the EU level."[58]

Another core issue exists surrounding the concepts of purpose limitation and data minimisation. These concepts play a significant role in discovering a potential balance between industry goals and individual data subject rights.

The GDPR principle of purpose limitation,[59] with its origins in international standards developed by the OECD[60] and the Council of Europe,[61] reflects the rights articulated in Article 8(2) of the Charter of Fundamental Rights of the European Union as follows:

> *"These data must be processed fairly, for specified purposes, and with the consent of the individuals to which they relate or on the basis of some other legitimate basis laid down by law."*

The GDPR principles of data minimisation[62] and storage limitation[63] are linked to purpose limitation in that no more data may be collected or processed, kept in a form that permits identification, or stored for longer than necessary for the purpose stated at the time of collection. Both in the past and continuing at present, processing in identifiable form when not required, and questionable further (or secondary) processing of personal data, including indefinite storage routinely occurs as an assumed by-product of the primary purpose for which the data was collected.

Under GDPR Article 6(4), personal data collected and processed for a stated purpose on the basis of Legitimate Interests, a contract or vital interests – *i.e., not based on consent* – may be further processed for another purpose only if the new purpose is compatible with the original purpose. The following points are highlighted in GDPR Article 6(4) as being relevant for determining whether a new purpose is compatible with the original purpose:

- the link between the original purpose and the new/upcoming purpose;
- the context in which the data was collected (what is the relationship between a data controller and the individual?);
- the type and nature of the data (is it sensitive?);
- the possible consequences of the intended further processing (how will it impact the individual?);
- the existence of appropriate safeguards (such as encryption or pseudonymisation).[64]

GDPR Article 6(4) highlights that if a data controller has collected the data on the basis of consent or following a legal requirement, no further processing beyond what is covered by the original consent or the provisions of the law is possible. In these instances, "further processing would require obtaining new consent or a new legal basis."

This underscores the "Hobson's Choice" noted above: if the processing is too complex to explain simply, (or too complicated to comprehend, but data subjects consent anyway, rendering the consent invalid) then either the processing cannot be allowed at all (with the attendant loss of societal benefits from the processing) or a non-consent legal basis must, in practice, actually be available for use.

For these reasons, we respectfully request that the EDPB confirm the capabilities of properly implemented GDPR-compliant pseudonymisation as a means of "tipping the balance in favour of Legitimate Interests processing" to enable

lawful and trusted processing leveraging complex data analysis, AI, ML, sharing, combining, and enriching not otherwise supportable using consent or contract.[65]

III.B - Heightened GDPR Requirements for Pseudonymisation

The GDPR provides incentives to use technical and organisational measures, including pseudonymisation, to enable the flow, commercial use, and value maximization of data in a way that recognizes, respects, and enforces the fundamental rights of individuals while allowing for the benefits to society from the use of data.

As noted by European Data Protection Supervisor, Wojciech Wiewiórowski, during the EDPS webinar, "Pseudonymous Data: Processing Personal Data While Mitigating Risks:

> *"Our legal data protection rules in the European Union and particularly GDPR itself considered pseudonymisation as a sort of model of all risk mitigating measures. This comes only after the first of all obligations, if you do not need the personal data do not process them. But if you need the personal data, then GDPR refers to pseudonymisation when it takes exemplifying the appropriate safeguards in many circumstances."*[66]

Before the GDPR, pseudonymisation was widely understood to mean replacing direct identifiers with tokens and was applied to individual fields independently within a data set. It was merely a privacy enhancing technique.

The definition of pseudonymisation in GDPR Article 4(5) requires that the information value of data must be separated from the identity of data subjects and that additional securely stored information must be necessary to re-identify data subjects, and then only under controlled conditions. **It is critical to note that under this new definition, GDPR-compliant pseudonymisation is now defined as an outcome for a data set and not (merely) a technique.**

With the elevation of pseudonymisation to an outcome, achieving GDPR-compliant pseudonymisation requires protecting not only direct identifiers but also indirect identifiers. In addition, instead of being applied only to individual fields, GDPR-defined pseudonymisation, in combination with the GDPR definition for Personal Data,[67] now requires that the outcome must apply to a data set as a whole (the entire collection of direct identifiers, indirect identifiers and other attributes), and consideration must be given to the degree of protection applied to all attributes in a data set.

As a result, pre-GDPR approaches (using a static token on a direct identifier, which unfortunately is still widely and incorrectly referred to as "pseudonymisation") will rarely, if ever, meet the heightened GDPR requirements of pseudonymisation. This also means that old approaches known as "pseudonymisation" will not be sufficient to meet the new heightened requirements under EU law.

III.B.1 - Requested Confirmation: GDPR Article 4(5) Definitional Requirements

Accordingly, we respectfully request confirmation by the EDPB that the GDPR Article 4(5) definitional requirement:[68]

> *"…that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person…"*

(1) Makes reference to an outcome for a dataset as a whole, not just treatment of individual fields in isolation, and

(2) Requires more than mere possession by the data controller or other authorised party of information enabling reidentification. Instead, this statutory language requires that **technical and organisational measures** (such as those identified in III.B.2 below) are **implemented making it impracticable** for third parties to identify an individual **without access to the additional information** held separately by the data controller or other authorised party.

III.B.2 - Requested Confirmation: Requirements for Use Case 2: Transfer of Pseudonymised Data[69]

Thomas Zerdick, Head of Technology and Privacy at the EDPS stated that:

> *"After the Schrems II ruling, the debate on pseudonymisation has gained momentum as many consider it as the most viable 'supplementary measure' to transfer personal data to third countries not offering an equivalent level of protection."*[70]

Accordingly, we respectfully request confirmation by the EDPB of the following standards for GDPR-compliant pseudonymisation under the EDPB Schrems II Recommendations[71] for satisfying Schrems II requirements for supplementary measures:

- **Protecting all data elements**: Footnotes 83 and 84 of the EDPB Schrems II Recommendations 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 as a whole, including more than direct identifiers, and 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 Schrems II Recommendations requires 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 Schrems II Recommendations to protect against the use of information from different datasets to re-identify data subjects necessitates the use of different replacement tokens for differing purposes at different times (i.e., dynamism) to prevent re-identification by leveraging correlations among data sets without needing access to the "additional information held separately" by the EU data controller (see https://www.MosaicEffect.com);

- **Non-algorithmically derived lookup tables**: the requirement of Paragraph 89 of the EDPB Schrems II Recommendations 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-algorithmically derived look-up tables in many instances; and

- **Controlled relinkability**: The combination of the four preceding items are necessary to meet the requirement in Paragraph 85(1) of the EDPB Schrems II Recommendations 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."

III.C - Benefits of GDPR Compliant Pseudonymisation

Monir Azraoui, Technology Expert with the CNIL, stated that:

> *"Data Controllers may not be aware that the GDPR encourages the use of pseudonymisation. I think that there are more than sixteen (16) occurrences of pseudonymisation in the GDPR. And they are not aware that pseudonymisation helps to reduce the risks associated with processing data and can help relax some GDPR obligations."*[72]

Organisations engage in Unprotected Processing by Default because of its processing efficiency and the significant shortcomings of traditional methods for protecting data when in use during computation and analysis,[73] which suffer from:

- Limitation to centralized or enclave processing (e.g., Differential Privacy).

- High processing overhead and/or bandwidth requirements (e.g., Homomorphic Encryption and Multi-Party Computing).
- Value degradation (e.g., Synthetic Data).
- Limited use cases (e.g., Contract-based protections limit use cases to those expressly required for the contracted product or service).
- Inability to relink to identity for authorised processing (e.g., Synthetic Data).
- Time intensive manual (bespoke) approval processes that extend the time necessary to review proposed data use projects and reduce the number of projects that get approved.

In contrast, properly implemented GDPR-compliant pseudonymisation:

- Supports both centralized and decentralized processing (centralized controls over decentralized processing).
- Requires no special processing overhead or bandwidth requirements (equivalent requirements to processing identifying cleartext data).
- Involves no value degradation (100% precision compared to identifying cleartext data).
- Does not limit use cases (see attached Exhibit 1 for discussion of Legitimate Interest-based processing with pseudonymisation-enabled technological controls).
- Supports controlled relinking to identity for the benefit of data subjects for authorised processing.
- Enables automation of key privacy enforcement processes (by reducing time for privacy reviews by 75% and increasing the number of projects approved by 4X to deliver up to 16X improved speed to insight).[74]

See also attached Exhibit 2 for comparative technical and performance benefits of properly implemented GDPR-compliant pseudonymisation versus PETs.

To encourage greater use of pseudonymisation (i.e., “Practicably Protected Data” as defined herein) versus Unprotected Processing by Default (as defined herein), we respectfully request confirmation by the EDPB of the following GDPR statutory benefits that are possible when processing properly implemented GDPR-compliant pseudonymisation:

III.C.1 - Requested Confirmation: Lawful Processing in US Operated Public Clouds

The Schrems II ruling, in combination with the EDPB Schrems II Recommendations and 2021 EC SCCs, make it clear that with limited exceptions, the processing of identifying cleartext regarding EU data subjects is no longer lawful when using US cloud service providers – regardless of the location of the data centers involved.[75] However, the processing of data that has been properly pseudonymised to GDPR requirements is lawful provided the information necessary to reattribute the information to data subjects is under the exclusive control of an EU Data Controller as required under EDPB Use Case 2[76] so the data is “surveillance proof.”

III.C.2 - Requested Confirmation: Availability of Schrems II Derogations

GDPR-compliant pseudonymisation helps to enable lawful international transfer and processing of global data including EU personal data by establishing by default the processing of protected GDPR-compliant pseudonymised data whenever, wherever, and as often as possible (as required by GDPR Articles 25 and 32) to ensure protected processing within the control of the EU Data Controller (a Data Embassy[77] 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 under Article 6 (e.g., based on Article 6(1)(a) consent, 6(1)(b) contract, 6(1)(f) legitimate interests, or 9(2)(j) scientific research by leveraging GDPR pseudonymisation-enabled technical and organisational measures to satisfy the "Balancing of Interests" test); 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 Schrems II Recommendations to enable repetitive use for specific situations.[78]

III.C.3 - Requested Confirmation: Lawful Data Repurposing, Sharing and Combining

Lawful Repurposing, Sharing and Combining. Pseudonymisation is explicitly highlighted in GDPR Article 6(4)(e) as an "appropriate safeguard" that can be used by data controllers "in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected."[79]

III.C.4 - Requested Confirmation: Legitimate Interest Processing When Consent and Contract are Not Appropriate

a. Properly pseudonymised data is recognized in the WP29 Opinion 06/2014 as **playing "…a role with regard to the evaluation of the potential impact of the processing on the data subject...tipping the balance in favour of the controller" to help support Legitimate Interest processing to protect data in use.**[80]

b. See attached Exhibit 1 for discussion of Legitimate Interest-based processing with pseudonymisation-enabled technological controls.

c. The benefits of processing personal data using compliant Legitimate Interests processing as a legal basis under the GDPR include:

   i. Under Article 17(1)(c), if a data controller can show they "have overriding legitimate grounds for processing" supported by technical and organizational measures to satisfy the Balancing of Interests test, they have greater flexibility in complying with Right to be Forgotten requests.

   ii. Under Article 18(1)(d), a data controller has flexibility in complying with requests to restrict the processing of personal data if they can show they have technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the fundamental rights of the data subject are protected.

   iii. Under Article 20(1), data controllers using Legitimate Interests processing are not subject to the right of portability, which applies only to consent-based processing.

   iv. Under Article 21(1), a data controller using Legitimate Interests processing may show they have adequate technical and organizational measures in place so that the rights of the data controller properly override those of the data subject because the fundamental rights of the data subjects are adequately protected. However, data subjects always have the right under Article 21(3) *to not receive* direct marketing outreach resulting from such processing.

III.C.5 - Requested Confirmation: Special Category Processing

a. Pseudonymisation may help to satisfy the Article 9(2)(g) exception to the general prohibition against the processing of special category data if the "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

b. Pseudonymisation may help to satisfy the Article 9(2)(i) exception to the general prohibition against the processing of special category data if the "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."

c. Pseudonymisation may help to satisfy the Article 9(2)(j) exception to the general prohibition against the processing of special category data if the "processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) [which explicitly cites pseudonymisation] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

III.C.6 - Requested Confirmation: Relaxation of Certain Re-Identification Obligations

a. Pseudonymisation helps to enable Article 11(2) relaxation of obligations to data subjects under GDPR Articles:

- 15 - Right of Access by Data Subject,
- 16 - Right to Rectification,
- 17 - Right to Erasure - Right to be Forgotten,
- 18 - Right to Restriction of Processing,
- 19 - Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing, and
- 20 - Right to Data Portability,

when processing does not require identification, if the data controller is not in the position to identify data subjects and the controller has informed data subjects accordingly. Data controllers not in possession of "Additional Information" necessary for re-identification would satisfy this requirement.[81]

b. Pseudonymisation helps to enable Article 12(2) relaxation of obligations under GDPR Articles:

- 15 - Right of Access by Data Subject,
- 16 - Right to Rectification,
- 17 - Right to Erasure - Right to be Forgotten,
- 18 - Right to Restriction of Processing,
- 19 - Notification Obligation Regarding Rectification or Erasure of Personal Data or Restriction of Processing, and
- 20 - Right to Data Portability,

in addition to the relaxation of obligations under GDPR Articles:

- 21 - Right to Object to Automated Decision-Making) and
- 22 - Automated Individual Decision-Making, Including Profiling),

to provide transparent information, communication, and modalities for the exercise of the rights of the data subject if the data controller can demonstrate it is not in a position to identify data subjects. Data controllers not in possession of "Additional Information" necessary for re-identification would satisfy this requirement.

III.C.7 - Requested Confirmation: Privacy-Respectful Profiling and Digital Marketing

a. Pseudonymisation may help to reduce the risk that profiling "produces legal effects concerning [data subjects] or similarly significantly affects [data subjects]" under Article 22(1) if it is left up to the data subject whether to choose to participate in opportunities presented to them as a member of a properly implemented pseudonymised group.

b. Pseudonymisation may help to reduce the risk that profiling "decision[s are made] based solely on automated processing" under Article 22(1) if it is left up to the data subject whether to choose to participate in opportunities presented to them as a member of a properly implemented pseudonymised group.

c. Pseudonymisation may help to enable Article 22(2)(b) support for processing "authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests."

d. Pseudonymisation may help to enable Article 22(4) allowance for decisions "based on special categories of personal data referred to in Article 9(1)" premised on Article 9(2)(g) Union or Member State laws by ensuring that "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place."

III.C.8 - Requested Confirmation: Data Protection by Design and by Default Obligations

a. Article 25(1) requires data controllers - for both primary and secondary processing - to "implement appropriate technical and organisational measures, **such as pseudonymisation**." (Emphasis added.)

b. Pseudonymisation helps data controllers to satisfy their obligations under Article 25(2) to "implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."[82]

III.C.9 - Requested Confirmation: Security and Data Breach Obligations

a. Article 32 explicitly recognises pseudonymisation and encryption as measures to be considered when "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."[83]

b. Pseudonymisation helps to ensure that data breaches are "unlikely to result in a risk to the rights and freedoms of natural persons." This would mean that an incident would not qualify as a data breach under GDPR and thus would not have to be notified to a supervisory authority under Article 33, nor be communicated to data subjects under Article 34.[84]

III.C.10 - Requested Confirmation: Data Protection Impact Assessments

a. Pseudonymisation may help to satisfy Article 35(3)(b) obligations for "processing on a large scale of special categories of data referred to in Article 9(1)."

b. Pseudonymisation may help to satisfy that the Article 35(8) creation of and adherence to "approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment."

c. Pseudonymisation may help to enable Article 35(10) elimination of separate data protection impact assessment obligations under Articles 35(1)-(7) "[w]here processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis."

III.C.11 - Requested Confirmation: Expanded Lawful Processing

a. Article 89(1) provides that "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include Pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

b. Article 89(1) Pseudonymisation-enabled processing enables greater flexibility under GDPR Articles:

- 5(1)(b) regarding purpose limitation,
- 5(1)(e) regarding storage limitation, and
- 9(2)(j) regarding overcoming the general prohibition on processing Article 9(1) special categories.[85]

III.D - Lawfulness of Combining EDPB Schrems II Recommendations and 2021 EC SCCs

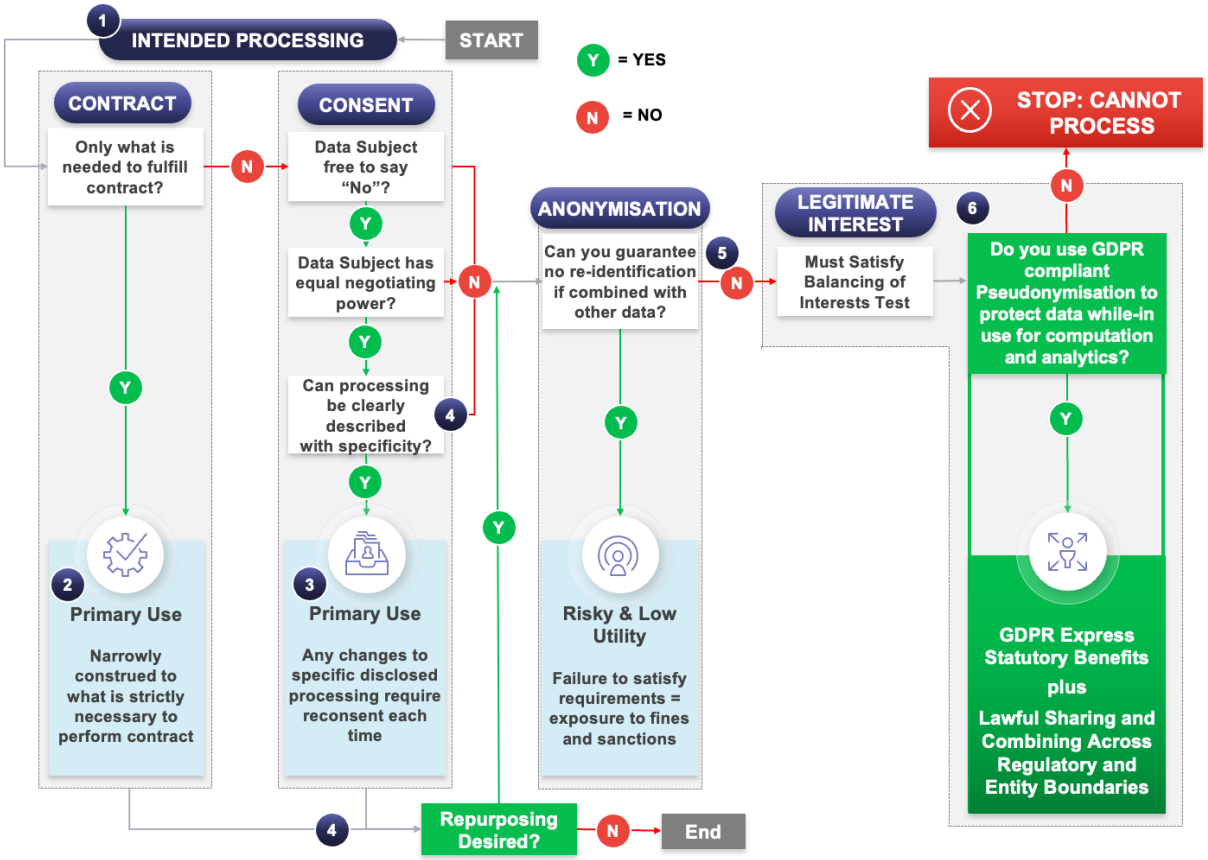
To address the considerable uncertainty faced by data controllers and processors, we respectfully request confirmation by the EDPB of the interim lawfulness of using the 2021 EC SCCs with the supplementary measures recommended in the EDPB Schrems II Recommendations pending EC and EDPB agreement on what supplemental SCCs should include when a data importer is subject to the GDPR.

ANONOS

Exhibit 1

Legitimate Interests Processing with Pseudonymisation-Enabled Controls

The following graphic and accompanying narrative highlight the differences in the suitability of contract, consent, anonymisation and GDPR pseudonymisation-enabled Legitimate Interest processing to support repurposing of data for secondary processing, including personalization.



Marketing Example:

Number references below correspond to number references in the graphic above

1. Examples of Intended Purposes

   - Sell a trip via a website (flight, hotel, etc.)
   - Save preferences for future bookings
   - Market analytics to offer personalized future trips via email

2. Under Contract

   - Can sell initial trip, but cannot (a) save for future bookings or (b) market for future trips

3. Under Consent

   - Can save preferences for future bookings within scope of consent only

- Works only for lawful marketing analytics which are disclosed with specificity at time of initial data collection

4. New marketing is (a) secondary repurposing under Contract and (b) fails requirements of advanced specificity for Consent and thus “further processing would require obtaining new consent or a new legal basis.”

5. Due to the details of the data collected and the need to retain indirect identifiers and attributes unprotected to perform desired analytics, the requirements for anonymisation under the GDPR are not satisfied.

6. Legitimate Interest is the remaining applicable option for a legal basis for lawful and ethical marketing analytics, artificial intelligence (AI) and machine learning (ML). GDPR-compliant pseudonymisation can help to provide protection for data while in-use computation for analytics, AI and ML to help tip the balance in favor of processing by the data controller.

ANONOS

Exhibit 2

Comparative Technical and Performance Benefits of GDPR-Compliant Pseudonymisation

Classification			Evaluation & Elimination Criteria				
			①	②	③	④	⑤
Privacy Enhancing Technologies (PET)	**Non-Cryptographic Techniques**	**Cryptographic Techniques**	**Protects Data In Use During Computation and Analysis**	**Supports Accurate Detailed Results at Record-Level**	**Reconciles Conflicts Between Protection and Utility**	**Supports Artificial Intelligence (AI) and Machine Learning (ML)**	**Supports Protected Data Sharing and Multi-Cloud Processing**
Encryption		✓	NO				
Differential Privacy	✓		YES	NO			
Cohorts/Clusters	✓		YES	NO			
Masking	✓		YES	YES	NO		
Generalization	✓		YES	YES	NO		
Hashing/Tokenization	✓		YES	YES	NO		
K-Anonymity	✓		YES	YES	NO		
Noise Introduction	✓		YES	YES	NO		
Synthetic Data	✓		YES	YES	NO		
Multi-Party Computing (MPC)		✓	YES	YES	YES	NO	
Homomorphic Encryption (HE)		✓	YES	YES	YES	NO	
Trusted Execution Environment (TEE)/ Confidential Computing Environment (CCE)		✓	YES	YES	YES	YES	NO
GDPR-Compliant Pseudonymisation	✓	✓	YES	YES	YES	YES	YES

Note: Once eliminated, PETs are not evaluated against subsequent criteria

The above chart compares a wide range of privacy enhancing technologies (PETs). After listing them, they are classified as using either cryptographic or non-cryptographic techniques (or in the case of pseudonymisation, both).

The balance of the chart to the right is a “knock-out” analysis of the technologies using a series of evaluation and elimination criteria. In this analysis, once a PET has been eliminated, it is no longer evaluated against subsequent criteria.

The first criteria in column (1) is protection of data during computation for uses such as analytics, AI and machine learning. This is sometimes called protection in use, to contrast it with protection of data at rest and in transit. Encryption is the de facto standard for protection of data at rest and in transit, but is successful at doing so precisely because it renders data unusable for computation and does not protect data when in use.

The second criteria in column (2) considers the ability of the PET to provide results that deliver detailed record level protection. Differential Privacy and cohorts/clusters by definition provide aggregate results rather than record level results and thus fall out at this point.

The third criteria in column (3) looks at how well a PET succeeds at delivering effective protection, while preserving utility comparable to processing cleartext. Each of the PETs receiving a “No” evaluation suffers from an inability to resolve a fundamental tradeoff between protection and utility. Greater protection invariably results in a loss of utility and preservation of utility results in weaker protection, regardless of whether the approach adds noise, masks or generalizes values, or synthesizes artificial data.

The fourth criteria in column (4) involves the ability of a PET to efficiently and effectively support AI and machine learning. Multi-party computing fails in this regard as a result of massive bandwidth requirements to coordinate calculations between participating nodes. Similarly, homomorphic encryption is not computationally feasible at the time and data volume scales required by these analytical techniques. And any future advances in computation power will still always leave them orders of magnitude slower than other PETs, which will also benefit relative to today’s performance from the additional computational power and speed.

The fifth criteria in column (5) looks at the ability of the remaining options to enable data-sharing and multi-cloud use cases. Confidential Computing via a Trusted Execution Environment, which has fared well up to this point now also drops out, as by its nature, the trusted execution environments that are used to achieve confidential computing are by design impenetrable silos, antithetical to data sharing.

At this point, the remaining PET is GDPR pseudonymisation which simultaneously:

- Protects data during computation for analytics
- Provides accurate (vs cleartext) record-level results
- Reconciles the trade-off between protection and utility
- Supports AI and machine learning
- Supports data sharing and multi-cloud use cases

ANONOS

Appendix

Reconciling Data Use and Protection
Pseudonymisation-Related Webinars & Presentations

Title	Date	Speakers	Highlights of Webinar	Replay Link
Schrems II Webinar: Technical Supplementary Measures: Surviving and Thriving Under Schrems II	June 22, 2021	• Polly Ralph, Director and Privacy Lawyer - **PwC UK** • Sarah Pearce, Partner - **Paul Hastings** • Magali Feys, Founder & Data Protection Lawyer - **AContrario.Law** • Gary LaFever, CEO & General Counsel - **Anonos**	The impact of Schrems II on the new EU-US Trade and Technology Council (TTC) and the capabilities of GDPR Pseudonymisation.	https://www.anonos.com/webinar-replay-schrems-ii-webinar-survive-and-thrive-under-schrems-ii
Top Ten Truths About GDPR Pseudonymisation	May 17, 2021	• Steffen Weiss, Legal Counsel - **German Association for Data Protection and Data Security (GDD)** • Gary LaFever, CEO & General Counsel - **Anonos**	Ten truths regarding what Pseudonymisation is (and is not) and how it enables you to achieve GDPR compliance and derive business benefits.	https://www.anonos.com/top-ten-truths-about-gdpr-pseudonymisation
Future Proofing Your Business for Evolving Privacy Laws	March 24, 2021	• Glenn Brown, Of Counsel - **Squire Patton Boggs** • Jill Reber, General Manager - **Logic 20/20** • Gary LaFever, CEO & General Counsel - **Anonos**	Learn how lessons learned from the GDPR help you to prepare for US Data Privacy laws.	https://www.anonos.com/webinar-future-proofing-your-business
Life After Privacy Shield - Strategies for Lawful Transfers of Personal Data from EU Countries to the U.S.	March 18, 2021	• Ashley Gorski, Staff Attorney - **ACLU** • Leo Moore, Partner - **William Fry** • Christian Hammerl, Executive Committee - **CA Bar Privacy Law** • Gary LaFever, CEO & General Counsel - **Anonos**	Enable affected businesses to make better decisions in their efforts to comply with EU data export regulations.	https://www.anonos.com/webinar-life-after-schremsii
Briefing the C-Suite & Board of Directors on Schrems II Risk Exposure	February 18, 2021	• Dr. Gabriela Zanfir-Fortuna, VP for Global Privacy - **FPF** • Magali Feys, Founder & Data Protection Lawyer - **AContrario.Law** • Gary LaFever, CEO & General Counsel - **Anonos**	How to brief C-Suites & Boards of Directors on Schrems II risk exposure. Evaluate the need for prompt action to establish an immediate defensible solution.	https://www.anonos.com/briefing-the-c-suite-board-of-directors-on-schrems-ii-risk-exposure
Schrems II: Implementation Roadmap & Legal Benefits	January 13, 2021	• Magali Feys, Founder & Data Protection Lawyer - **AContrario.Law** • Gary LaFever, CEO & General Counsel - **Anonos**	Achieving predictability of operations. Schrems II Impact on International Data Transfers.	https://AContrario.Law/implementation-workshop-replay
Schrems II Lawful Cloud Processing and SCCs	October 29, 2020	• Dr. Gabriela Zanfir-Fortuna, VP for Global Privacy - **FPF** • John Bowman, Senior Principal - **Promontory** • Mark Webber, US Managing Partner - **Fieldfisher** • Patrick Van Eecke, Partner - **Cooley** • Magali Feys, Founder & Data Protection Lawyer - **AContrario.Law** • Gary LaFever, CEO & General Counsel - **Anonos**	Lawful cloud processing. Standard contractual clauses. What additional safeguards exist.	https://www.schremsii.com/cloud-webinar-replay
Schrems II Lawful Data Transfers	October 8, 2020	• Anna Buchta, Head of Policy & Consultation Unit – **EDPS** • Romain Robert, Senior Lawyer - **NOYB** • John Bowman, Senior Principal - **Promontory** • Mark Webber, US Managing Partner - **Fieldfisher** • Patrick Van Eecke, Partner - **Cooley** • Magali Feys, Founder & Data Protection Lawyer - **AContrario.Law** • Gary LaFever, CEO & General Counsel - **Anonos**	What to expect in follow up to the Schrems II decision by the CJEU.	https://www.schremsii.com/edps-noyb-webinar-replay-transcript
Saving Direct Marketing in the Post-Pandemic Economic Recovery	April 30, 2020	• Christopher Docksey, Honorary Director General - **EDPS** • Marc M. Groman, Principal - **Groman Consulting Group** • Dave Cohen, Knowledge Director - **IAPP** • Gary LaFever, CEO & General Counsel - **Anonos**	The Role of Robust Pseudonymisation Controls Under the GDPR	https://www.anonos.com/direct-marketing-webinar-post-pandemic-recovery
Legitimate Interest Microsegmentation - Based Direct Marketing	April 16, 2020	• Christopher Docksey, Honorary Director General - **EDPS** • Martin Abrams, Chief Strategist - **Information Accountability Foundation** • Dr. Sachiko Scheuing, European Privacy Officer - **Acxiom**	Discussion about Legitimate Interest Microsegmentation-based Direct Marketing under the GDPR	https://www.anonos.com/functional-separation-legitimate-interest-direct-marketing-webinar
Pseudonymisation-Enabled Legitimate Interest Processing	March 19, 2020	• Martin Abrams, Chief Strategist - **Information Accountability Foundation** • Dr. Sachiko Scheuing, European Privacy Officer - **Acxiom** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about Legitimate Interest processing under the GDPR	https://www.anonos.com/legitimate-interest-processing-webinar

ANONOS

Appendix
(Continued)

Reconciling Data Use and Protection
Pseudonymisation-Related Webinars & Presentations

Title	Date	Speakers	Highlights of Webinar	Replay Link
Can Pseudonymisation Save AdTech: Pseudonymisation and the 5th Cookie Initiative	February 13, 2020	• Martin Abrams, Chief Strategist - **Information Accountability Foundation** • Paul Comerford, Principal Technology Policy Advisor - **ICO** • Dr. Sachiko Scheuing, European Privacy Officer - **Acxiom** • Dave Cohen, Knowledge Director - **IAPP** • Gary LaFever, CEO & General Counsel - **Anonos**	While highlighting AdTech, the webinar covers how GDPR compliant Pseudonymisation can enable lawful and ethical data use under the GDPR generally.	https://www.anonos.com/iapp-webinar-pseudonymisation-adtech
Legitimate-Interest Processing under the GDPR	January 23, 2020	• Ailidh Callander, Legal Officer - **Privacy International** • Dave Cohen, Knowledge Director - **IAPP** • Rocco Panetta, Managing Partner - **Panetta & Associati** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about how to satisfy the legal and technical requirements for Legitimate Interests processing under the GDPR	https://www.anonos.com/iapp-legitimate-interest-webinar-v2
CPDP: Technical & Organizational Controls for Lawful AI & Secondary Processing When Consent is Not Enough	January 23, 2020	• Ailidh Callander, Legal Officer - **Privacy International** • Giuseppe D'Acquisto, Senior Technology Advisor – **Italian Garante** • Steffen Weiss, Legal Counsel - **German Association for Data Protection and Data Security (GDD)** • Magali Feys, Founder & Data Protection Lawyer - **AContrario.Law** • Gary LaFever, CEO & General Counsel - **Anonos**	Overview of technical and organisational controls for lawful AI and secondary processing under the GDPR	https://www.anonos.com/cpdp-gdpr-lawful-ai-and-secondary-processing
What to Do When Consent Doesn't Work	January 16, 2020	• Deven McGraw, Chief Regulatory Officer - **Ciitizen** • Khaled El Emam, Professor - **University of Ottawa** • Justin Antonipillai, Founder & CEO - **WireWheel** • Dave Cohen, Knowledge Director - **IAPP** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about available options under US and EU law when consent requirements cannot be satisfied	https://www.anonos.com/iapp-webinar-when-consent-does-not-work
Lawful Repurposing and Sharing of Data	November 14, 2019	• Nasya Bennacer, Head of Financial Services - **Hitachi Vantara** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about unlocking maximum data utility using Digital Privacy Variant Twins	https://www.anonos.com/warsaw-presentation-2019
Introduction to Fair Trade Data - Balancing Innovation and Data Privacy	May 25, 2019	• Günther Leissler, Partner - **Schoenherr** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about "Fair trade Data" as a means of balancing innovation and data privacy	https://www.anonos.com/fair-trade-data-webinar-1
BigPrivacy GDPR Webinar	July 15, 2018	• Francois Zimmerman, Global CTO - **Hitachi Vantara** • Gary LaFever, CEO & General Counsel - **Anonos**	Is Data minimization killing off your Big Data projects? How does your firm handle cross-border data consolidation?	https://www.anonos.com/hitachi-bigprivacy-webinar-july
5G and GDPR: Just Because You Can Capture Data Does Not Mean You Can Use It	May 17, 2018	• Dr. Alison Knight, Data Governance Lead - **University of Southampton** • Gary LaFever, CEO & General Counsel - **Anonos**	Learn how new dynamic data protection requirements under the GDPR can help to resolve these conflicts and help to facilitate adoption of 5G capabilities.	https://www.anonos.com/5g
Just Because You're GDPR Compliant Does Not Mean You Can Use Your Data	April 18, 2018	• Dr. Alison Knight, Data Governance Lead - **University of Southampton** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about the difference between baseline GDPR compliance and the requirement to protect data during processing for use to be lawful	https://www.anonos.com/iapp-london-video-replay
Briefing On GDPR Compliant Data Analytics	January 30, 2018	• Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about requirements for protecting data during processing for lawful data use under the GDPR	https://www.anonos.com/hitachi-breakfast-briefing-on-compliant-data-analytics
CPDP: Data Protection by Design and by Default	January 24, 2018	• Dr. Alison Knight, Data Governance Lead - **University of Southampton** • Gwendal Le Grand, Director of Technology and Innovation - **CNIL** • Malte Beyer-Katzenberger, Policy Officer - **DG CONNECT** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about the importance of technical solutions for GDPR-compliant Data Protection by Design and by Default	https://www.anonos.com/cpdp-the-importance-of-technical-solutions-such-as-dynamic-pseudonymous-data

ANONOS

Appendix
(Continued)

Reconciling Data Use and Protection
Pseudonymisation-Related Webinars & Presentations

Title	Date	Speakers	Highlights of Webinar	Replay Link
Don't Lose Access to Data Analytics Under the GDPR	September 20, 2017	• Gwendal Le Grand, Director of Technology and Innovation - **CNIL** • Jules Polonetsky, CEO - **Future of Privacy Forum (FPF)** • Gary LaFever, CEO & General Counsel - **Anonos**	The GDPR Increases Options for Organizations to Process Data. Support for Global Data-Driven Business Beyond GDPR Compliance. Controlled Re-Linking of Data Increases the Value of Data Analytics.	https://www.anonos.com/gdpr-data-analytics-webinar-replay
GDPR Innovation Briefing	July 19, 2017	• Wojciech Wiewiórowski, Assistant Supervisor – **EDPS** • Martin Abrams, Chief Strategist - **Information Accountability Foundation** • Hilary Wandall, Chief Data Governance Officer - **TrustArc** • Gary LaFever, CEO & General Counsel - **Anonos**	Discussion about how the GDPR is structured to enable innovation	https://www.anonos.com/gdpr-innovation-webinar-replay
IAPP Bring Your Own Legal Basis (BYOB) Under GDPR	April 19, 2017	• Gary LaFever, CEO & General Counsel - **Anonos**	The technical prerequisites for supporting lawful data use under the GDPR	https://www.anonos.com/iapp-summit-byob-bring-your-own-legal-basis
GDPR Big Data Analytics Webinar	March 8, 2017	• Gwendal Le Grand, Director of Technology and Innovation - **CNIL** • Mike Hintze, Partner - **Hintze Law** • Gary LaFever, CEO & General Counsel - **Anonos**	"Consent" and "Contract" do not support analytics, AI or ML. GDPR requires more than privacy by design - it mandates data protection by design and by default. Data assessments and inventories alone or not enough. Encryption alone does not support analytics, artificial intelligence or machine learning using personal data.	https://www.anonos.com/gdpr-big-data-iapp-industry-faqs
How to Comply with the GDPR While Unlocking the Value of Big Data	January 31, 2017	• Gwendal Le Grand, Director of Technology and Innovation - **CNIL** • Mike Hintze, Partner - **Hintze Law** • Gary LaFever, CEO & General Counsel - **Anonos**	The GDPR Increases options for organizations to process data. Support for global data-driven business beyond GDPR compliance. Controlled re-linking of data increases the value of data analytics.	https://www.anonos.com/iapp-gdpr-data-analytics-webinar-replay

[1] Magali Feys is Chief Strategist of Ethical Data Use at Anonos and founder of AContrario Law, a boutique law firm based in Belgium 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 Chief Executive Officer and General Counsel at Anonos, Global Innovator at the World Economic Forum, former partner at the law firm 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 and 80+ additional patent assets internationally.
[3] See https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en
[4] References to "Schrems II" refer to 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
[5] See Lomas, *In Bad News For US Cloud Services, Austrian Website's Use Of Google Analytics Found To Breach GDPR*, at https://techcrunch.com/2022/01/12/austrian-dpa-schrems-ii/
[6] See GDPR Recitals 78 and 108 and Article 25.
[7] The term "Unprotected Processing by Default" refers to the widespread business practice of processing EU personal data in the clear and in formats that are readily re-linkable, thereby exposing the identities of EU citizens; see Section III.A below for further definition.
[8] See page 38 at https://noyb.eu/sites/default/files/2022-01/E-DSB%20-%20Google%20Analytics_EN_bk.pdf
[9] See https://edps.europa.eu/ipen-webinar-2021-pseudonymous-data-processing-personal-data-while-mitigating-risks_en
[10] See https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf
[11] GDPR Recital 78 stipulates that "The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible…."
[12] The first recital of the GDPR states that "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her."
[13] See Appendix - Reconciling Data Use and Protection, Pseudonymisation-Related Webinars & Presentations
[14] See https://www.linkedin.com/groups/12470752/
[15] See Manancourt, *With Amazon Fine, Luxembourg Emerges As Europe's Unlikely Privacy Champion*, at https://www.politico.eu/article/amazon-fine-luxembourg-europe-privacy-champion/
[16] See Lomas, *Grindr's $7M GDPR Fine Is A Stark Warning To Adtech Not To Track*, at https://techcrunch.com/2021/12/15/grindr-final-gdpr-fine/
[17] See Lomas, *France Latest To Slap Clearview AI With Order To Delete Data*, at https://techcrunch.com/2021/12/16/clearview-gdpr-breaches-france/
[18] See Lomas, *IAB Europe's Ad Tracking Consent Framework Found To Fail GDPR Standard,* at https://techcrunch.com/2020/10/16/iab-europes-ad-tracking-consent-framework-found-to-fail-gdpr-standard/
[19] See Supra Note 5.
[20] See Lomas, *European Parliament Found To Have Broken EU Rules On Data Transfers And Cookie Consents*, at https://techcrunch.com/2022/01/10/edps-decision-european-parliament-covid-19-test-website/
[21] See page 34 at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[22] See page 35 at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[23] See https://edps.europa.eu/ipen-webinar-2021-pseudonymous-data-processing-personal-data-while-mitigating-risks_en
[24] See https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[25] See https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en
[26] See https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en
[27] See Recital 7 of the EU Commission's Implementing Decision which states: "A controller or processor may use the standard contractual clauses set out in the Annex to this Decision to provide appropriate safeguards within the meaning of Article 46(1) of Regulation (EU) 2016/679 for the transfer of personal data to a processor or controller established in a third country, without prejudice to the interpretation of the notion of international transfer in Regulation (EU) 2016/679. The standard contractual clauses may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation (EU) 2016/679. This also includes the transfer of personal data by a controller or processor not established in the Union, to the extent that the processing is subject to Regulation (EU) 2016/679 (pursuant to Article 3(2) thereof), because it relates to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union."
[28] See Lokke and van der Wolk, *Why it is Unlikely the Announced Supplemental SCCs will Materialize*, at https://iapp.org/news/a/why-it-is-unlikely-the-announced-supplemental-sccs-will-materialize/ citing Kuner, "*The GDPR, A Commentary*," on pg. 758.
[29] Id.
[30] Paragraph 76 of EDPB Schrems II Recommendations highlights the obligations of controllers and processors to implement the same measures described as Supplementary Measures therein to comply with GDPR requirements with respect to personal data

processed in the EEA (citing GDPR Article 5 (which includes keeping personal data "in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed") and Article 32 (which specifically highlights pseudonymisation). Paragraph 83 of EDPB Schrems II Recommendations similarly highlights the obligation of controllers and processors to implement the same measures described as Supplementary Measures therein when data is processed by a data importer covered by an equivalency decision or in the EEA (citing Articles 25 and 32, which both specifically highlight pseudonymisation).

[31] Paragraphs 5, 15 and 17 of Guidelines 05/2021 highlight that although data flows may not constitute transfers under Chapter V, such processing can still be associated with risks for which safeguards must be envisaged. Regardless of whether the processing takes place in the EU or not, controllers and processors must always comply with all relevant provisions of the GDPR.

[32] See 5:04 at https://edps.europa.eu/press-publications/press-news/videos/ipen-2021-pseudonymous-data-keynote-speech-wojciech_en.

[33] GDPR Recital 78 stipulates that "The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible…."

[34] See paragraph two on page three at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

[35] See 11 October 2021 "Embracing Heightened Standards for Anonymisation and Pseudonymisation" memorandum at https://www.anonos.com/ico-anonymisation-pseudonymisation-comment-letter, including the following quote: "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."

[36] Id, including the following UK references to/definitions of pseudonymisation: "Safeguards such as techniques that make it less easy to identify individuals from data sets (generically known as pseudonymisation techniques)" and "[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."

[37] Id.

[38] See GDPR Article 4(5) definition of pseudonymisation which requires "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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

[39] GDPR Recital 26 of the GDPR 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". This 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 necessary and the means to re-identify. Footnote 2 in Annex II of the 2021 EC SCCs stipulates 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." In addition, Paragraphs 79, 85, 86, 87 and 88 of the EDPB Schrems II Recommendations highlight that you must consider the availability of external data sets enabling unauthorised re-identification.

[40] It is interesting to note that in the context of concluding that the Personal Information Protection Act (as updated, "PIPA") ensures an adequate level of protection for EU personal data processed by controllers and processors in the Republic of Korea, the EC highlighted that instead of relying on pseudonymisation as a possible safeguard, PIPA imposes it as a non-elective precondition for certain processing activities pertaining to statistics, scientific research and archiving in the public interest (such as to be able to process the data without consent, perform further processing or to combine different datasets). See paragraphs 36 and 42 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf ("South Korea Adequacy Decision") and PIPA Sections 15(1), 28(2) and 28(3).

[41] See https://edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en

[42] Privacy International; see https://privacyinternational.org/sites/default/files/2018-11/08.11.18 Final Complaint Acxiom %26 Oracle.pdf at 28.

[43] Johnny Ryan, chief policy officer at Brave; see https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate

[44] IAB, see https://www.iab.com/wp-content/uploads/2020/02/IAB_The-Great-Collab_ALM-2020-Keynote-Script.pdf at 8

[45] Eduardo Ustaran - Hogan Lovells Privacy and Cybersecurity Practice Global Co-Head; see https://iapp.org/news/a/critics-on-croatias-eprivacy-proposal-legitimate-interest-provisions-not-legitimate

[46] See Moerel & Prins, *Privacy For The Homo Digitalis: Proposal For A New Regulatory Framework For Data Protection In The Light Of Big Data And The Internet Of Things*, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123 ("Privacy For The Homo Digitalis") at 9.

[47] World Economic Forum Report: Unlocking the Value of Personal Data: From Collection to Usage, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf at 11.

[48] Koops, "The trouble with European Data Protection Law," International Data Privacy Law, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692 at 4. See also Supra Note 44 *Privacy For The Homo Digitalis*.

[49] See Dutch Minister of Economic Affairs in a letter on Big Data and Profiling. Parliamentary Documents II, 2014/15, 32761, nr. 78, p. 4.

[50] See https://www.merriam-webster.com/dictionary/Hobson%27s%20choice

[51] See EDPB Guidelines 5/2020 at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[52] See Article 29 Working Party Opinion on the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC, currently under revision by the EDPB (see the EDPB Work program 2021/2022 adopted on the 16 March 2021)

[53] See EDPB Recommendations 02/2021on page 3 at https://edpb.europa.eu/system/files/2021-05/recommendations022021_on_storage_of_credit_card_data_en_1.pdf citing CJEU judgement of 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme', Case C-13/16, ECLI:EU:C:2017:336
[54] Id, citing CJEU judgement of 11 December 2019, TK v Asociaţia de Proprietari bloc M5A-ScaraA, Case C-708/18, ECLI:EU:C:2019:1064
[55] Id.
[56] Id, citing CJEU judgement of 24 November 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado, Cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, points 47 and 48; CJEU judgement of 19 October 2016, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779
[57] See Article 29 Working Party 06/2014 at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf at 35.
[58] See Supra Note 46, *Privacy For The Homo Digitalis* citing Case C-131/12 Google Spain and Google Inc. May 13, 2014, EU:C:2014:317; Case C-362/14, Schrems, October 6, 2014, EU:C:2015:650; Opinion WP29 06/2014.
[59] GDPR Article 5(1)(b).
[60] See Section 9 of the OECD, 1980: "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."
[61] See Article 5(b) of the Council of Europe, 1981.
[62] GDPR Article 5(1)(c).
[63] GDPR Article 5(1)(e).
[64] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that under PIPA pseudonymisation is a non-elective precondition for GDPR Article 6(4) equivalent further processing for statistics, scientific research and archiving in the public interest. See paragraph 36 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Section 15(1).
[65] See GDPR Articles 5(1)(a), 6(1)(f), and Opinion 06/2014 on the notion of legitimate interests of the data controller at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[66] See *https://edps.europa.eu/press-publications/press-news/videos/ipen-2021-pseudonymous-data-keynote-speech-wojciech_en at 4:06*
[67] GDPR Article 4(1) defines Personal Data as "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."
[68] GDPR Article 4(5) defines pseudonymisation 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 organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."
[69] 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
[70] See https://edps.europa.eu/press-publications/press-news/videos/ipen-2021-pseudonymous-data-introduction-thomas-zerdick_en at 4:00
[71] 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
[72] See https://edps.europa.eu/press-publications/press-news/videos/ipen-2021-pseudonymous-data-monir-azraoui_en at 5:36
[73] Encryption as used by organisations for many years only protects data when at rest and in transit, leaving data exposed when in use during computation and analysis, resulting in "Unprotected Processing by Default." See Exhibit 2 for Comparative Technical and Performance Benefits of GDPR-Compliant Pseudonymisation.
[74] Performance results are based on the experience of parties using Anonos Data Embassy GDPR pseudonymisation software. See https://www.anonos.com/
[75] For more information, see https://www.linkedin.com/pulse/updated-schrems-ii-top-5-faqs-lawful-cloud-processing-gary-lafever/
[76] See EDPB Schrems II Recommendations 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
[77] See https://www.anonos.com/edpb-memorandum. See also Italian university dissertation on using GDPR pseudonymisation for purposes of creating "Data Embassies" for purposes of Schrems II compliance is available at https://www.schremsii.com/epilogue. Data Embassy is also a trademark of Anonos.
[78] See "Expanded Flexibility for Derogations" on page 11 (internal page 2) of the consolidated university dissertation regarding Schrems II at www.anonos.com/UniversitySchrems2Ddissertation
[79] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that instead of relying on pseudonymisation as a possible safeguard, under PIPA it is a non-elective precondition for certain processing activities pertaining to statistics, scientific research and archiving in the public interest (such as to be able to process the data without consent, to perform Article 6(4) equivalent repurposing or to share or combine datasets). See paragraphs 36 and 42 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Sections 15(1), 28(2) and 28(3).
[80] See pages 42 and 67 at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
[81] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that PIPA prohibits the processing of pseudonymised information with the purpose of identifying a certain individual. In fact, if information that could identify an individual would be generated while processing pseudonymised information, the controller must immediately suspend the processing and destroy such information. "Failure to comply with these provisions is subject to administrative fines and constitutes a criminal offence. This means that, even in those situations where it would be practically possible to re-identify the individual, such re-identification is legally prohibited." See paragraphs 44 and 82 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Sections 28(5) and 28(7).

[82] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that pseudonymisation is a non-elective precondition under PIPA for certain processing activities pertaining to statistics, scientific research and archiving in the public interest (such as to be able to process the data without consent, repurposing, sharing and combining datasets). See paragraphs 36 and 42 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Sections 15(1), 28(2) and 28(3).
[83] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that parties have an affirmative obligation under PIPA to "endeavour to process personal data in anonymity or in pseudonymised form, if possible." See paragraph 62 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Sections 3(6) and 3(7).
[84] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that under PIPA parties are not required to notify individuals when a data breach involves pseudonymised information processed for the purposes of statistics, scientific research or archiving in the public interest. See footnote 87 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Section 28(7).
[85] It is interesting to note that the EC highlighted in the South Korea Adequacy Decision that the obligation to destroy personal data upon achieving the purpose of processing or upon expiry of the retention period (whichever is earlier), does not apply under PIPA when pseudonymised data is processed for statistical purposes, scientific research or archiving in the public interest. See paragraph 60 at https://ec.europa.eu/info/sites/default/files/1_1_180366_dec_ade_kor_new_en.pdf and PIPA Section 21(1).

EDPBmemo@anonos.com