ULD - ENISA WORKSHOP: PSEUDONYMISATION & RELEVANT SECURITY TECHNOLOGIES

Date: November 12, 2019

Location: Berlin, Germany

Website: https://www.enisa.europa.eu/events/uld-enisa-workshop/uld-enisa-workshop-pseudonymization-and-relevant-security-technologies

ENISA, the European Union Agency for Cybersecurity, and the Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), the Data Protection Authority of the German Federal State of Schleswig-Holstein, co-organised a workshop on "Pseudonymisation and relevant security techniques" on November 12, 2019 in Berlin.

The main objective of the workshop was to advance existing debates on the deployment of pseudonymisation solutions as a means to meet GDPR requirements and data controller/processor obligations. To this end, the workshop aimed to discuss and touch upon core pseudonymisation techniques, practical approaches and existing application instantiations along to legal and economic issues. Attendance to the workshop was available on an invitation basis, so as to promote an open and lively dialogue among experts in the field.

This report provides the main points and key messages as presented by speakers and participants of the workshop.

WELCOME MESSAGES

The workshop was opened by Marit Hansen, Data Protection Commissioner of Land Schleswig-Holstein and ENISA's Athena Bourka, who welcomed the participants and explained the main objectives of and motivations for the workshop on behalf of the two co-organisers. The importance of bringing research and policy together in the field of pseudonymisation was particularly emphasised, especially in the context of specific application scenarios that can be analysed in practice. Marit Hansen further stressed the need to raise awareness as regards the benefits of pseudonymisation techniques, while engaging professionals from different disciplines/backgrounds in this discussion (from lawyers and policy makers, to computer scientists and IT technicians).

SESSION 1 – TECHNIQUES AND EXPERIENCES SO FAR

Steffen Weiß (German Association for Data Protection and Data Security - GDD)

Steffen Weiß started his intervention by laying out key questions surrounding pseudonymisation, namely its definition, main benefits and requirements. He noted that there is a common

misinterpretation of pseudonymisation with anonymisation. When data controllers apply pseudonymisation techniques, they have made an informed decision that the data will be pseudonymised with the potential of being re-identified in the future. Another misunderstanding can be caused by considering encryption as pseudonymisation. Encryption can be part of a pseudonymisation process but cannot be considered as pseudonymous data. Mr Weiß defined pseudonymisation as a security control to protect the data subject. He suggested that there is a protective aspect on pseudonymisation (art.32 par.1 l.a GDPR), but further thought should be given on how pseudonymisation can complement privacy by design and by default principles. Also, Mr Weiß argued on the enabling function of pseudonymisation for personal data processing in view of art. 6 par.1 l.f and art.6 par.4 l.e GDPR. Additional difficulties rise from eliciting requirements to effectively deploy pseudonymisation. There is a transformation process to allow organisations to apply in tandem technical security controls (i.e., access control mechanisms) and controls to ensure transparency when processing data.

Mr Weiß further presented GDD's work in the field, starting from a white paper on pseudonymisation (2017), which mainly focused on raising/describing the relevant issues, followed by another paper with guidelines/requirements in 2018. Based on this work, in 2019 the first draft Code of Conduct (CoC) on pseudonymisation was published. As identified in the draft CoC, there are several challenges as regards the operationalisation of pseudonymisation. These include ensuring the lawfulness of data processing, information of data subject for further processing by third parties, application of data subjects rights to pseudonymous data, re-identification of data subjects (which might be needed for a number of reasons). The most difficult problem is to identify the best possible technique, based on risk (to the data subject).

Mr Weiß argued that it is impossible to prescribe a specific pseudonymisation technique in a universal CoC. To this end, the methodology suggested in the paper starts by assigning responsibilities to controllers/processors so as to be in control establishing, implementing and reviewing the process of pseudonymisation. Organisations need to think of the types of risk associated with the data they hold, the purpose of processing this data, the context of processing, the data sets (dynamic, many datasets), the types of pseudonyms (will define the risk of re-identification) and the privacy by default or design principles. Once this exercise is documented, there are further checkpoints regarding: the transferring of the data (there is no additional information such as metadata); transferring of data to third countries; access control mechanisms (with additional information on identifying the data subject); controls that rely on third parties (document accountability regarding in-house or outsourcing of these controls); necessity of processing (do organisations need the pseudonymous data or not); transformation requirements and risk practices (key length, structure of raw data).

Overall, the CDD CoC does not prescribe mandatory requirements for pseudonymisation but provides minimum technical requirements such as the level of entropy and types of hash functions to be used. Finally, the issue of local vs global anonymisation/pseudonymisation was discussed by Mr Weiß (how can additional information reveal the identity of data subjects). The German approach is to focus the risk approach on local criteria.

Nils Gruschka (University of Oslo)

Mr Gruschka started his intervention with the definition of pseudonymisation and the notion of pseudonyms and elaborated on a number of architectures for pseudonymisation, inter alia, directly replacing the pseudonym, third parties being involved, chained pseudonymisations with mappings. While doing so he provided some examples from the field of medical research where it is common to conduct research on the actual medical data or on pseudonymised data (i.e., patient data, samples). He then proceeded with describing the requirements for a range of techniques used in pseudonymisation, such as one time use of pseudonymisation only, with no interest in re-identification, or cases with harder requirements such as follow up on patient's records (which requires a mapping between the patient's name and the pseudonym). The latter case is where the re-identification of a patient is mandatory (notification of a serious disease) requiring organisations to apply bidirectional mapping.

Mr Gruschka briefly identified techniques on how a pseudonym can be created. A simple technique is to provide random numbers as pseudonyms (with a certain length, no identifier repeated etc.), which allows a bidirectional mapping. Organisations could also design a counter or use symmetric encryption (using a symmetric key, storing only the secret key). Alternatively, the use of cryptographic hash-function can be opted, which does not require storing of a key and allows a single direction mapping (from patient to pseudonym only). Finally, there is the cryptographic hash function, which stores a key.

Mr Gruschka concluded his talk by exploring attacks on pseudonymity that can be performed by an insider or an external attacker. The main assumption is that organisations need a mapping table to re-identify a data subject. However, with additional information, people may perform attacks by identifying rare or unique cases in the pseudonymised data (i.e., someone from small village with a broken leg).

Achim Klabunde (European Data Protection Supervisor - EDPS)

Achim Klabunde started his presentation with the definition of pseudonymisation (article 4 GDPR), pointing out that pseudonymisation is often confused with the notions of encryption, de-identification, and anonymization. He described the differences between these terms and explained that, from a data protection point of view, they are fundamentally different.

Focusing on the GDPR definition, Mr Klabunde stressed that the data subject may be "identified" or "identifiable", and that the legislator considers the use of "additional information". He also noted that, while GDPR encourages the use of pseudonymisation, there is no silver bullet as to its application (reference to recital 26 GDPR, which states that all available means need to be considered by the data controller when determining whether a person is identifiable). This also points to the practical difficulties of pseudonymisation, as the controller does not control all means that can be used for attacks against pseudonymisation (e.g. data being processed or derived by other entities for the same data subjects).

Mr Klabunde mentioned the recent guidelines on hash functions published by AEDP (Spanish DPA) and EDPS, as a way to provide practical guidance on the implementation of pseudonymisation techniques to data controllers.

Discussion

Discussion revolved around the terms that can be used to describe the secret part of pseudonymisation (e.g. key or mapping table depending on the technique applied or "additional information" under GDPR). This topic raised a broader discussion about terminology and the importance to evaluate methods and solutions for pseudonymisation. Participants distinguished between absolute (global) and relative (local) pseudonymisation. Opinions as to this perception vary but workshop participants in general agreed that the risk-assessment process of GDPR is inherent in this approach (and the controllers can identify the risks only based on the data/information they have in their disposal).

SESSION 2 – TECHNIQUES AND EXPERIENCES SO FAR

Giuseppe d'Acquisto (Garante - Italian DPA)

Giuseppe d'Acquisto started his presentation by highlighting the risks from ineffectively implementing pseudonymisation. Organisations erroneously assume that pseudonymised data can increase the ways in which they can be processed. However, this approach "opens the pandora's box" instead of increasing the security posture of an organisation. With the use of simple examples, Mr d'Acquisto argued that organisations that apply recklessly article 4 par.5 of GDPR, may result in revealing sensitive personal information. A key factor in these examples was context, which suggests that there is not an absolute characteristic in pseudonymisation that can be applicable everywhere.

Mr d'Acquisto explained that as individuals, we have multiple identities depending on the different contexts/parts of our lives. Pseudonymisation is the way to manage these identities and introduces a characteristic of relativity. We should rebuild our mind to see what is important whenever we reveal information. The effective implementation of data-protection principles through pseudonymisation can mitigate the likelihood of additional data revealing personal information.

Technical features that can help in implementing successfully pseudonymisation include: inversion of pseudonymisation to be proved computationally impossible, unintelligible output of humans but not machines, negligible collision probability, output distance insensitive with regards to input distance (small differences in the number of characters provide bigger differences in the output).

Mr d'Acquisto particularly pointed to pseudonymisation's role in supporting data integrity. For example, integrity and accuracy are increased with the use of hash functions (due to increasing the distance when few characters are changed). However, computational irreversibility is not panacea because additional information, based on the context, can re-identify an individual. Therefore, irreversibility of a function is not by default the best way to ensure confidentiality without additional controls in place.

Lastly, Mr d'Acquisto referred to zero proof knowledge algorithms for pseudonymisation (as means for data minimisation and the implementation of erasure in context where data are persistent and broadly available, like for instance distributed ledgers technologies). He also stressed that pseudonymisation reinforces lawfulness and, therefore, relevant controls on its correct implementation should be foreseen.

Monir Azraoui (CNIL - French DPA)

Mr Azraoui started his presentation by reference to the usual misunderstanding around pseudonymisation and anonymisation. He explained that people confuse anonymisation with pseudonymisation because they do not follow the essential criteria to design anonymous datasets (i.e., singling out, correlation, inference). A main difference is that the pseudonymised data are within the scope of GDPR and are still considered personal data. Most data controllers want to reach the state of anonymised data to avoid implications from GDPR, as they see it as a burden and not an opportunity. The challenge of pseudonymisation is how to facilitate the data subjects' rights (access, erasure, portability mentioned in Article 11.2).

Mr Azraoui continued by describing bad practices of unsuccessfully implementing pseudonymisation that CNIL has observed over the last few years. These include: hashing (without key) as an anonymisation mechanism; removal of the direct identifier; usage of weak cryptographic keys; use of obsolete algorithms; no technical measures to protect secret keys; and inadequate measures to protect against additional information.

Mr Azraoui also provided examples of good practices for pseudonymisation. These include: performing re-identification risk analysis; protection of secret key used in pseudonymisation; and combining pseudonymisation with other security measures (encryption of pseudonymised files stored and in transit).

CNIL has imposed sanctions in cases where poor pseudonymisation was performed. These range from a warning, to formal notice and finally to a sanction (injunction under a coercive fine). Sanctions can be public or remain confidential.

Finally, Mr Azraoui presented examples where organisations, with the help of CNIL, have successfully completed projects in pseudonymisation. The techniques used where tailored for the needs of the organisations and were context-depended. The first example demonstrated how a local authority used pseudonymisation to outsource the scanning of sensitive records to a non-EU country. The technique consisted in splitting the records into several pieces, each processed by distinct persons. The second example presented how the French health insurance information system estimates the expenses of the French health system in a privacy-friendly manner. There is a general regime and many smaller special regimes with their separate databases. Two level pseudonymisation is performed; the first level is performed at the source where hash functions pseudonymise the gender, the security number and the date of birth. The second level pseudonymises the collected pseudonymised data. The pseudonyms allow the French authorities to analyse the data without access to personal information of the individuals. The last example was the ticket validation data in public transportation systems, used to mitigate fraud. A cryptographic

hash function is applied and the secret key is frequently refreshed and cannot be directly accessible by a single user. It was emphasised that all these solutions were implemented before GDPR came into force.

Bud P. Bruegger (ULD - Schleswig-Holstein DPA)

Mr Bruegger argued for the need of a widely accepted terminology on pseudonymisation. When reasoning about pseudonymisation there is a lack of accepted terminology and a clash between technical and legal terms. Personal data consists of data records that link to people directly or indirectly. GDPR provides a structure on what data are considered personal and these data entail identifiers and identity specific factors. Identifiers can be probabilistic or unique. Mr Bruegger introduced a (technical) data pseudonymisation term to distinguish this notion from GDPR's definition of pseudonymisation. He further explained that when organisations consider personal data, the first step is to distinguish identifying elements from other presumed data. The second step is to shred parts of the identifying data and create pseudonyms for the rest of the identifying data. Then the remaining data must be anonymised.

There are three possible ways of identifying persons based on pseudonymised data. Under well-defined conditions, controllers can use the additional information to re-identify persons behind pseudonyms. In addition, attackers can in certain cases invert the pseudonym (using brute force) or acquire external additional information that can link to the person in question.

Pseudonyms enable the linking of related data that belong to the same data subject. The strategy followed for pseudonymisation will control the extent to which such links exist (single pseudonym per person, multiple pseudonyms per person).

Mr Bruegger concluded his talk by announcing a paper that will be published soon with the aim to establish standard terminology that also includes the technical concepts that are missing in the GDPR.

Discussion

Participants discussed that pseudonymisation is a process where the identity of a person is concealed and provides mechanisms to revert this process. The impact (of reversal of pseudonymisation) is an important criterion for the applicability of certain pseudonymisation methods. The discussion revolved around whether pseudonymisation can reduce the impact of a data breach. Participants concurred that, in principle, pseudonymisation would play an important role in reducing the impact but suggested organisations to conduct periodical risk assessments on how additional information may give rise to re-identification attacks.

SESSION 3 – APPLICATION SCENARIOS

Meiko Jensen (Kiel University of Applied Sciences)

Meiko Jensen presented (on behalf of the relevant ENISA's working group) ENISA's latest work on pseudonymisation techniques and best practices. The first issue the report aimed to tackle was the problem with definitions for pseudonymisation processes, as well as the entities and the

adversaries involved in these processes. Mr Jensen described the roles that relate to GDPR and coined term for the equivalent to encryption secret key for pseudonymisation.

Mr Jensen continued with a number of scenarios from ENISA's report where controllers and processors perform a variety of activities that involve pseudonymisation. He elaborated on a number of adversary models and the techniques encountered in these examples. Pseudonymisation techniques that were reported include counter, random number generator, cryptographic hash functions, Hash Mac (secret key) and symmetric encryption; other advanced techniques were briefly mentioned (e.g., Merkle trees, Bloom filters, pseudonymisation chains). The scope of pseudonymisation was considered to estimate different pseudonymisation policies (deterministic, document-random), as well as the dilemma between data protection and utility.

To validate the aforementioned pseudonymisation techniques, Mr Jensen presented two different cases considered in the ENISA's report. For the IP address pseudonymisation, different utility scenarios were considered to decide on the appropriate pseudonymisation technique that will increase the utility of data in this scenario. The second case study focused on data for email addresses. The debate in this scenario was how to preserve utility while enhancing security. The question revolved on whether organisations should pseudonymise the whole email address or just the part that follows the @ symbol.

Mr Jensen concluded that pseudonymisation is a risk-based approach without an optimal technique that applies to all scenarios. To this end, there is no single solution for pseudonymisation that would work for all possible scenarios and further analysis on specific application scenarios is needed in practice.

ENISA's report is available in: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

Frank Wagner (Deutsche Telekom AG)

Frank Wagner presented the approach that Deutsche Telekom AG has institutionalised to anonymise or pseudonymise data. Mr Wagner described a risk assessment approach, which is based on a three-coloured scheme for estimating the impact of personal data being realised. The red domain consists of raw data that the lowest possible number of users will have access. The amber contains data, which have been anonymised or pseudonymised. These data are aggregated and updated periodically. Finally, the green area contains data, which is deemed non-critical allowing access rights to all users. There is a continuous process in place to evaluate the criticality of data in these areas.

Mr Wagner shared examples of how anonymised or pseudonymised data are used in practice. The first case is the design of an anonymised dataset to create insights of statistical nature for public transport planning and tourism (i.e., how many people get off on a specific tube station). Anonymisation is achieved by considering all available data that the organisation holds before aggregating different data fields. Once the aggregation of data is concluded, data extrapolation techniques follow (only 1/3 of the market is covered by Deutsche Telekom) therefore, the danger

of re-identification is further reduced. There is a periodical process in place to estimate the risk of de-anonymising the aggregated data.

For the second case, Mr Wagner described an IPTV service named Mangenta TV. This service contains a recommendation function which utilises pseudonymisation to create datasets based on which TV shows are suggested to customers. Firstly, the pseudonymisation is performed on every customer's data (with salt/pepper techniques). Pseudonymised data are then aggregated to create statistics. These statistics are stored for 24 months and are used to provide suggestions for the viewers. Mr Wagner concluded by noting that pseudonymisation is a technique that should be tailored to organisational aspects.

Saffija Kasem-Madani (University of Bonn)

Saffija Kasem-Madani stipulated that pseudonymisation techniques, if not properly applied, on one hand do not guarantee privacy and on the other may destroy utility of data. Ms Kasem-Madani explained that she is partaking in a project where they collect personal data from different resources and they need to allow multiple analyses on the data (i.e., traffic in the city). Therefore, University of Bonn is considering pseudonymisation techniques to ensure users' privacy and utility for the desired analysis purpose when sharing their data for research purposes.

The core idea of the system that is designed is to enable the user to apply the pseudonymisation process. Therefore, the process of pseudonymisation must be simple, allowing practitioners to define how data should be used without explicitly identifying which technique has to be used for an appropriate utility-preserving pseudonymisation. The main premise requires pseudonyms to be automatically constructed based on a machine-readable description of utility requirements.. The pseudonyms are considered as sequences of utility tags. These tags are transformations of the plaintexts that allow for processing the desired utility. Each utility tag is associated with information on how the data will be utilised, described in a machine-readable format. Policy constraints are decided before the data are pseudonymised with a pseudonymisation function. The choice of which function will be applied to the data to produce the utility tags, depends on the purpose of processing of the data.
Among others, the techniques that are applied to produce utility tags include additive homomorphic encryption, deterministic cryptographic hashing and order-preserving encryption.

Overall, Ms Kasem-Madani stressed the need to apply analysis on pseudonymised data, therefore to strike the right balance between data protection and utility.

Patrick von Braunmühl (Bundesdruckerei GmbH - BDR)

Patrick von Braunmühl detailed BDR's approach to pseudonymising very sensitive data in the health sector. Health data, despite being a special category of data, is pertinent to be available for analysis. Pseudonymising such data raises several challenges because the researchers need to explore the chain of events and identify correlations between patients. Therefore, preserving utility is fundamental when pseudonymisation is performed.

BDR collects data from a variety of sources (hospitals, pharmacy, General Practitioners) and deploys pseudonymisation techniques before sharing the data for further analysis. The Trusted Data Platform offered by Bundesdruckerei comprises other functions such as identity and authorisation management, consent and access management as well as data quality assurance. The platform through which data is available for researchers enables them to run algorithms to obtain results, without ever the data leaving the database.

Mr von Braunmühl concluded his talk by referring to the Digital Supply Act, which was recently legislated in the German Parliament. The Act describes how health insurers should share data for research purposes. Insurances are obliged to pseudonymise datasets before data are shared and aggregated.

Fabian Prasser (BIH/ Charité for TMF)

Fabian Prasser focused on medical research and elaborated on the different types, such as controlled clinical trials, biobanking, population registries and health services research. Such diversity in research requires different data processing workflows and different data protection concepts to be in place. For certain types of research anonymised data is not an option. Therefore, pseudonymisation is at the heart of the data protection guidelines for medical research developed by TMF. The central idea behind pseudonymisation is to separate the storage of directly identifying data from the data needed for scientific analyses.

Additional paper-based processes, render the underlying data flows extremely complex (since pseudonyms can be printed on paper). There are several tools created by the medical informatics community to facilitate sharing of data by generating pseudonyms and managing identities in a protected manner.

Discussion

Participants acknowledged that there is a gap between what it is technically possible regarding pseudonymisation and what it is defined legally in GDPR. It was concurred that it is unfeasible to technically guarantee that the pseudonymised or anonymised data will not be subject to re-identification attacks. However, depending on the case, appropriate controls can be put in place to reduce the relevant risks. The definition of the state-of-the-art and practical use cases for pseudonymisation is essential to this end.

SESSION 4 – RESERCH AND LEGAL ISSUES

Simone Fischer-Hübner (Karlstad University)

Simone Fischer-Hübner presented a talk on choices of Implementation and end user challenges of configuration of pseudonyms.

Ms Fischer-Hübner started with an introduction to the concept of pseudonymisation based on two different taxonomies and a legal definition pursuant to Art. 4 par.5 GDPR. One taxonomy used to define pseudonyms was based on Pfitzmann and Hansen's seminal that allows to classify pseudonyms and their provided degree of (un-)linkability into a lattice structure based on the user

context. Another pseudomym taxonomy that was discussed is based on the type of revocability of pseudonyms and several examples of successful implementation of such complex process were given, inter alia, k-spendable pseudonyms (i.e. in elections to vote many times without revealing your identity), trusted id broker, secret sharing (k out of n actors), zero proof of knowledge, multi-level granularity and step wise.

From GDPR it transpires that encrypted data and sharing secrets classify as personal pseudonymous data. In order to securely store data in the cloud (i.e., image), Ms Fischer-Hübner explained that multiple fragments of an image can be stored in such a manner that k out of n are needed to be combined to rebuilt the picture (where k < n). Ms Fischer-Hübner pointed that secret sharing can be a solution for pseudonymisation and this principle was in the core of the design of the cloud-based secret sharing system.

The second part of the talk was based on use cases from the PRIMACLOUD EU project and addressed end user challenges for configuring such types of pseudonyms and for minimising data attributes associated with a user identity or pseudonym.

For configuring cloud-based secret sharing, different trade-off decisions need to be made for selecting parameters and storage nodes.
To elicit requirements for such a system, 16 structured interviews were conducted. Results suggest that it is difficult to establish the number k out of n server locations. Many participants would also not trust public cloud providers and opted for a hybrid approach (store locally data). Configuration settings providing suitable trade-offs should be provided for users based on the type of data to be protected.

Ms Fischer-Hübner elaborated on an e-health use case that enables users to selectively disclose authentic medical information associated with the user's identity. In this scenario, the doctor signs electronically a medical document with a malleable signature, passes it on to the patient, who can then, dependent on who should receive this information, redact parts of the original document, while the signature still stays valid. The challenge for the patient is how to enforce data minimisation without endangering his/her safety. The system depends on redaction templates with usability and trust factors considered to guide the redaction process.

Christian Geminn (Kassel University)

Christian Geminn reflected on Japan's approach to data protection to gain insights on how to further improve European practices. He argued that data controllers, due to the legal requirements set by GDPR, cannot ensure that globally all data related to a data subject will be identified, before pseudonymisation is applied. Therefore, since the risk of re-identification is a decisive factor on how pseudonymisation will be performed, organisations need to continuously monitor such risks. A possible solution to assure organisations that additional information will not sabotage the pseudonymisation of data is the existence of a trustworthy third party. This party will ensure that the data controller will not have legally or practically an option available to gain further information. If extremely sensitive data are involved, multiple pseudonymisation functions can be performed

(i.e., the hospital and a third party before providing – now effectively anonymised - data to researchers).

Mr Geminn continued by differentiating between anonymising pseudonymisation and risk reducing pseudonymisation. He provided the example of Japan, where a data protection regime came into force in 2017. This regime describes how anonymously processed information, similar to anonymised data, is created. It was introduced after companies insisted to have clear access to big data analysis.

The handling of personal data in Japan is generally described as over-prudent and heavily prohibiting data usage. The idea behind anonymously processed information is that data processing will be performed elevating risks regarding revealing personal data. Mr Geminn identified the requirements for the creation of such data and concluded with the security measures that a controller must deploy to protect such data. The anonymization method can remain with the controller as long as this information is stored separately.

CONCLUDING REMARKS

Based on the presentations and discussions throughout the workshop, the following concluding remarks can be drawn:

Different flavours of pseudonymisation or usage of pseudonyms

The definition on pseudonymisation (art. 4 par.5 GDPR) does not cover all flavours of what is being discussed under the term in the IT community. “Pseudonymisation of personal data by the controller” may be distinguished from the “usage of pseudonyms by data subjects”. Also, pseudonymisation is usually achieved by a combination of technological and organisational means; it goes beyond a mere mathematical function in a software component. Furthermore, related data minimisation techniques that do not exactly match the GDPR definition on pseudonymisation may still be valuable for reducing or mitigating risk as demanded by the GDRP. For the debate within or across different communities, clarification of the subject to be discussed is recommended.

Application scenarios

There is not a “one-fit-for-all” solution for pseudonymisation. While several techniques are available, their practical applicability depends highly on the context and the particular data processing scenario, as well as the underlying operational needs. Therefore, the community could greatly benefit from specific application scenarios in different sectors and for different types of personal data.

State-of-the-art

Further work needs to be conducted on the availability and practical implementation of advanced pseudonymisation techniques, e.g. those arising from the area of anonymisation. In this context,

the (sometimes) thin line between anonymisation and pseudonymisation needs to be explored (and maybe revisited).

Pseudonymisation and data subjects rights

An essential matter as regards pseudonymisation is the exercise of data subjects' rights, taking also into consideration art. 11 GDPR. Further examples and guidance for controllers would be highly beneficial to this end.